LCOS LX 7.20

Reference Manual

10/2026

ROHDE&SCHWARZ
Make ideas real

Contents

1 Introduction....6
1.1 Components of the documentation....6
1.2 LCOS LX, an operating system from R&S®NC....6
1.3 Validity....7
2 Operation....8
2.1 Configuration software....8
2.1.1 LANconfig – configuring devices....8
2.1.2 WEBconfig – monitoring and configuring devices....9
2.1.3 Command-line interface — command summary....10
3 Feature descriptions....15
3.1 WLC layer-3 tunnel....15
3.2 Band steering....15
3.3 Fast roaming....16
3.4 R&S®NC Enhanced Passphrase Security (LEPS)....17
3.5 WPA3 (Wi-Fi Protected Access 3)....18
3.5.1 WPA3-Personal....19
3.5.2 WPA3-Enterprise....20
4 Configuring features with LANconfig....21
4.1 Management....21
4.1.1 General....21
4.1.2 Admin....22
4.1.3 LMC....37
4.1.4 Extended....37
4.1.5 Software update....39
4.2 Interfaces....41
4.2.1 Port settings....42
4.2.2 Layer-3 Ethernet tunnel with L2TPv3....48
4.2.3 Multicast Snooping....50
4.2.4 DHCP Snooping....51
4.3 Date/Time....52
4.3.1 Configuration....52
4.4 IP configuration....55
4.4.1 LAN interfaces....56
4.4.2 Static parameters....57
4.5 Wireless LAN....58
4.5.1 WLAN networks....58
4.5.2 Wireless Distribution System (WDS) / point-to-point links....80
4.5.3 RADIUS....86
4.5.4 Client Management....87
4.5.5 Stations/LEPS....93

4.5.6 WLC....95
4.5.7 Firewall....99
4.5.8 End-to-End Test....102
4.6 IoT – the Internet of Things....109
4.6.1 Wireless ePaper....110
4.6.2 Bluetooth Low Energy (BLE)....114
4.6.3 USB....115
4.7 Other services....115
4.7.1 Location-based services (LBS)....115
5 Configuring features with WEBconfig....119
5.1 Commissioning of a device via WEBconfig....119
5.1.1 Management by R&S®LANCOM Management Cloud....121
5.1.2 Stand-alone management....121
5.2 Login....122
5.3 WEBconfig – Dashboard....123
5.3.1 Actions....123
5.4 Monitoring....125
5.4.1 Neighborhood....126
5.4.2 Bluetooth Low Energy....127
5.5 Wi-Fi configuration....128
5.5.1 Concept....128
5.5.2 Operation....128
5.5.3 WLAN users....139
5.5.4 WDS (Wireless Distribution System) / Point-to-point links....140
5.6 System configuration....146
5.6.1 Name....146
5.6.2 Security settings....147
5.6.3 SSH Public Key Authentication....147
5.6.4 Country settings....149
5.6.5 Time zone settings....149
5.6.6 Automatic firmware update....150
5.6.7 SNMP....152
5.6.8 Wi-Fi management....152
5.6.9 Wireless ePaper....154
5.6.10 Location based services....157
5.6.11 Network settings....159
6 Diagnosis....168
6.1 Trace output....168
6.1.1 Trace – an overview....168
6.1.2 Trace – operation....169
6.2 Logs in WEBconfig....169
6.3 Packet capturing in WEBconfig....169
6.4 Monitoring of Access Point Position and Mounting Angle....170
6.5 PoE Status Information....171

7 Factory default active services according to EN 18031 GEC-4.....173

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). All rights reserved.

Notice on the company name: Since July 1, 2026, LANCOM Systems has been named **Rohde & Schwarz Networks and Cybersecurity**. Product information and communication materials are accordingly issued under the new company name.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Rohde & Schwarz Networks and Cybersecurity 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 Rohde & Schwarz Networks and Cybersecurity. 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.

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under *gpl.rs-nc@rohde-schwarz.com*.

Products from Rohde & Schwarz Networks and Cybersecurity include software developed by the “OpenSSL Project” for use in the “OpenSSL Toolkit” (*www.openssl.org*).

Products from Rohde & Schwarz Networks and Cybersecurity include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from Rohde & Schwarz Networks and Cybersecurity include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from Rohde & Schwarz Networks and Cybersecurity contain the LZMA SDK developed by Igor Pavlov.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.rohde-schwarz.com/networks-and-cybersecurity

1 Introduction

1.1 Components of the documentation

The documentation of your device consists of the following parts:

Installation Guide

The Quickstart user guide answers the following questions:

- Which software has to be installed to carry out a configuration?
- How is the device connected up?
- How can the device be contacted with LANconfig or WEBconfig?
- How is the device assigned to the R&S®LANCOM Management Cloud?
- How do I start the Setup Wizard (e.g. to set up Internet access)?
- How do I reset the device?
- Where can I find information and support?

Quick Reference Guide

The Quick Reference Guide contains all the information you need to put your device into operation. It also contains all of the important technical specifications.

Reference manual

This Reference Manual goes into detail on topics that apply to a variety of models. The descriptions in the Reference Manual are based predominantly to the configuration with LANconfig.

Menu Reference Guide

The Menu Reference describes all of the parameters in LCOS LX. This guide is an aid to users during the configuration of devices by means of the CLI. Each parameter is described briefly and the possible values for input are listed, as are the default values.

All documents for your product which are not shipped in printed form are available as a PDF file from *Download-Bereich*.

1.2 LCOS LX, an operating system from R&S®NC

LCOS LX is the operating system for certain LANCOM access points and parts of the R&S®NC family of operating systems. The R&S®NC operating systems are the trusted basis for the entire R&S®NC product portfolio. Each operating system embodies the R&S®NC values of security, reliability and future viability.

- **Maximum security for your networks**

  as each LANCOM operating system is carefully maintained and developed in-house and with the accustomed quality. They are all guaranteed backdoor-free.

- **Reliability of the highest order**

  as they receive regular release updates, security updates, and major releases over their entire product lifetime.

› **Future viability for your networks**

according to the R&S®NC Lifecycle Policy, i.e. they are free of charge for all R&S®NC products and come with major new features.

1.3 Validity

The functions and settings described in this manual are not all supported by all models or all firmware versions.

2 Operation

2.1 Configuration software

There is no end of different situations in which configurations have to be carried out, or ways in which operators prefer to work. This is why the device offers a wide range of ways to set up the configuration:

- **LANconfig** – the menu-driven, clearly structured and easy way to set almost all parameters for a device. LANconfig requires a configuration PC with a current Windows operating system. Refer to the chapters *LANconfig – configuring devices* on page 8 and *Configuring features with LANconfig* on page 21 for further information.
- **WEBconfig** – further information can be found in the chapters *WEBconfig – monitoring and configuring devices* on page 9 and *Configuring features with WEBconfig* on page 119.
- **CLI** – as an alternative to LANconfig, you can also use SSH to open a terminal session on the device and access the command-line interface. TCP port 22 provides access to the device via SSH programs such as PuTTY.
- **R&S®LANCOM Management Cloud** – the hyper-integrated solution for automated control of your network.

The default credentials for all configuration paths are:

- User: root
- Password: <Empty> (no password is set)

In the interests of security, you will be prompted to change the password when you use WEBconfig to access the configuration for the first time.

Please note that all methods access the same configuration data.

2.1.1 LANconfig – configuring devices

From the easy commissioning of a single workplace device with convenient Installation Wizards to the overall management of large scale installations—the spectrum of applications for LANconfig is wide:

Basic functions

- Automatic detection of new, unconfigured devices
- (Remote) configuration of devices via IP address, URL, or via the serial interface
- Integration of Telnet, SSH, HTTPS and TFTP configuration
- Context-based help on the configuration parameters
- The Wizards provide customized input masks at every stage of installation
- Backup connection setup

Management of large installations

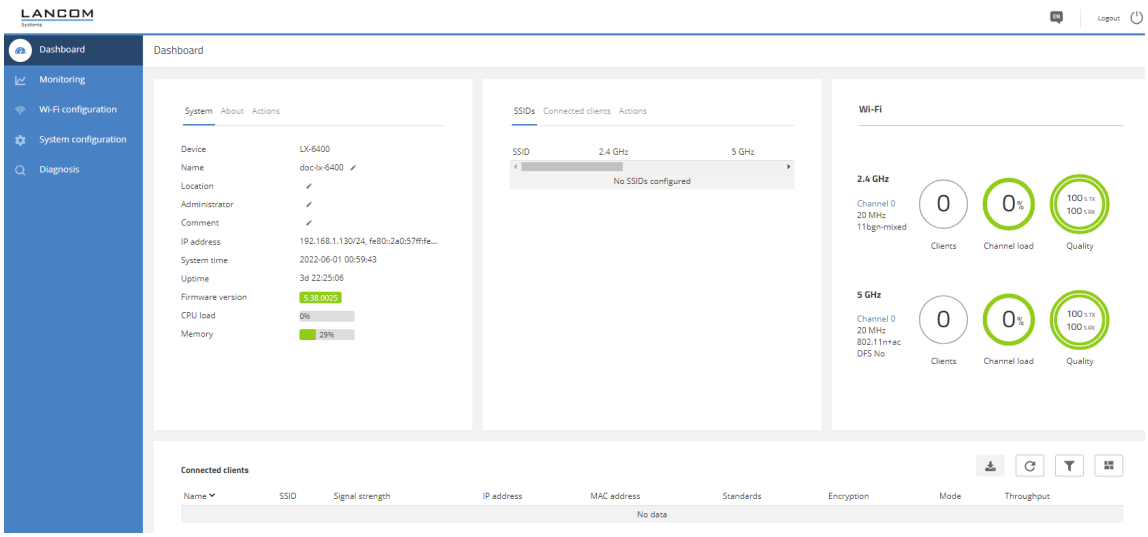
- Grouping
- Central firmware distribution
- Simultaneous configuration of multiple devices
- Configuration script distribution
- WLAN group configuration
- Logging of all actions
- Creation of new “offline” configurations for all devices, for LCOS, and for versions of LCOS LX

2.1.2 WEBconfig – monitoring and configuring devices

Using WEBconfig, you can configure individual devices or monitor them during operation. WEBconfig is reached via HTTP and HTTPS. If you use HTTP, the device automatically redirects you to an encrypted HTTPS connection.

WEBconfig uses a self-signed SSL certificate, so this must be added as an exception in the browser for each device.

The following provides an overview of the main components of WEBconfig, which are located in the left-hand section in the **sidebar**.



Dashboard

The Dashboard displays status information of the device during operation.

- System – basic information about the device, e.g. the device name and the firmware version.
- WLAN – information about the load on the WLAN channels operated by the device.
- Connected stations – shows all WLAN stations currently connected to the device.
- Neighborhood – overview of the WLAN environment, especially the WLAN access points and WLAN routers that are locally active.
- Monitoring – graphical representation of the WLAN throughput, LAN throughput, number of WLAN stations and channel load over time.

Configuration

- System configuration – configuration of basic parameters of your device, such as the device name or the IP settings for managing the device.

› WLAN – the WLAN configuration is designed to assist the user with the most common settings and to eliminate the hassle of configuring minor details. It remains possible to configure different scenarios.

Logs

This area outputs the device SYSLOG.

2.1.3 Command-line interface — command summary

The command-line interface is operated with the following commands. An overview of the available configuration parameters and actions is available in the LCOS LX Menu Reference Guide.

Which commands are available depends upon the equipment of the device.

For an overview of the available commands, just press the tab key twice. Enter the option `--help` after the command for an overview of the available parameters.

Changes to the configuration are not immediately boot-persistent. They have to be saved explicitly by using the command `flash`.

Table 1: Overview of all commands available at the command line

Command	Description
`add [<Path>]`	Adds a row to the table.
`beginscript`	Resets the CLI session to script mode. In this state, commands entered are not transferred directly to the device's configuration RAM but initially to its script memory. The mode is terminated by the command `exit`.
`cd <Path>`	Changes the current menu or directory.
`default`	Resets the table or the value to the default setting. This command works recursively. Therefore, all values and tables in the current path and those below it will be reset.
`del <Path> <Index>`	Deletes the value or the table row in the branch of the menu tree referenced by `<Path>`. Enter the line number for the `<Index>`.
`delete`	Synonymous with `del`.
`dir`	Synonymous with `ls`.
`do <Path> [<Parameter>]`	Executes the action in the current or referenced directory. If the action has additional parameters, they can be added at the end.
`exit`	Ends the terminal session.
`flash`	Store the configuration Changes to the configuration are not immediately boot-persistent. They have to be saved explicitly by using the command `flash`.
`history`	Displays a list of recently executed commands.
`ll2mdetect`	LL2Mdetect finds LL2M-capable devices in the network. The LL2M client uses this command to send a SYSINFO request to the LL2M server. The server then sends its system information, such as hardware and serial number, back to the client for display. The

Command	Description
	LL2Mdetect command can be restricted with the following parameters: **-a <MAC-address>** Restricts the command to those devices with the specified MAC address only. Enter the MAC address in the format `00a057010203`, `00-a0-57-01-02-03` or `00:a0:57:01:02:03`. If no MAC limitations are set, the "detect" is sent as a multicast (or alternatively using `-b` as a broadcast) to all LL2M-compatible devices. To contact groups of MAC addresses, `*` and `x` can be used as wildcards in individual MAC address positions, e.g., `00-a0-57-xx-xx-xx` for all device MAC addresses. In a command line with multiple parameters, the final parameter **must** be `-a`. A different order is not allowed. **-b** Explicitly sends the LL2Mdetect request as a broadcast and not as a multicast. **-f <Version>** Restricts the command to those devices with the corresponding firmware version only. **-r <Hardware-Release>** Restricts the command to those devices with the corresponding hardware release only. **-s <Serial number>** Restricts the command to those devices with the corresponding serial number only. **-v <VLAN-ID>** Only sends the LL2Mdetect request on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used. **A restriction of the command to a hardware type (with the parameter "-t") is not possible with LCOS LX.** The command `ll2mdetect -r A` sends a SYSINFO request to all devices of the hardware release "A". The response from the LL2M server then contains the following information:

Command	Description
	› Device name › Device type › Serial number › MAC address › Hardware release › Firmware version with date
`ll2mexec`	The command `ll2mexec` sends commands to or initiates terminal sessions on devices found by `ll2mdetect`. The LL2M client uses this command to send a single-line command to run on the LL2M server. Multiple commands can be combined in one LL2M command by using semicolons as separators. Depending on the command, the actions are run on the remote device and the responses from the remote device are sent to the LL2M client for display. The LL2Mexec command conforms to the following syntax: `ll2mexec -i <(W)LAN-Interface> <User>[:<Password>]@<MAC address>` The LL2Mexec command can be restricted with the following parameters: **`-i <(W)LAN-Interface>`** Sends the LL2Mexec command via the specified (W)LAN interface only. **`-v <VLAN-ID>`** Only sends the LL2Mexec command on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used. For example, the command line `ll2mexec -i ETH1 root@00a057010203 set /setup/name MyDevice` logs in the LL2M client as "root" on the LL2M server with the MAC address "00a057010203". Since the password was not included, the device first looks for the corresponding username in the local database and automatically uses the password for this user. If the username is also not included, the login data of the currently registered user for the CLI session is used. Then the LL2M client sets the name of the remote device to the value 'MyDevice'.
`list`	Synonymous with `ls`.
`ls [<Path>]`	Displays the contents of the current directory or path.
`passwd <Password>`	Changes the password of the current user account.
`ping [-c count] [-i interval] [-s packetsize] destination`	Sends an ICMP echo request to the IP address specified. Possible arguments are: › `-c count`: Send `count` pings. › `-i interval`: Time between packets in seconds. › `-s packetsize`: Sets the packet size to `packetsize` bytes (max. 65500). › `destination`: Address or host name of the target computer
`rm`	Synonymous with `del`.
`set <Index> {Column} <Value>`	Sets the value of a table row in a specific column to <Value>.

Command	Description
`set <Path> <Value(s)>`	Sets the value or values of a specific path to the specified value(s).
`show diag [<Parameter>]`	Output diagnostic information on the CLI.
`show 3rd-party-licenses`	Output the device license information on the CLI.
`startlmc <Activation Code> [Domain]`	After you have generated an activation code in the R&S®LANCOM Management Cloud, you use this code to pair the device with the R&S®LANCOM Management Cloud. You can optionally specify a new LMC domain as well.
`sysinfo`	Shows the system information (e.g., hardware release, software version, MAC address, serial number, etc.).
`trace [--log] [+|-|#|?] <Parameter>`	Starts (`+`) or stops (`-`) a trace command to output diagnosis data. `#` switches between different trace outputs and `?` displays a help text. The parameter `--log` restricts the output to “historical” log information. For further information on this command refer to the section *Diagnosis* on page 168.
`writeconfig [noflash]`	Writes a new configuration in the LCF file format to the device. The system interprets all of the following lines as configuration values until two empty lines are read. This is used by management systems, for example. Possible arguments are: › `noflash`: The transferred configuration is not persistent. This can be done subsequently by running the `flash` command.

Legend

› Characters and brackets:

  › Objects, in this case dynamic or situation-dependent, are in angle brackets.
  › Round brackets group command components, for a better overview.
  › Vertical lines (pipes) separate alternative inputs.
  › Square brackets describe optional switches.

  It follows that all command components that are not in square brackets are necessary information.

› `<Path>`:

  › Describes the path name for a menu or parameter, separated by "/".
  › `..` means: one level higher
  › `.` means: the current level

› `<Value>`:

  › Describes a possible input value.
  › `""` is a blank input value

› `<Name>`:

  › Describes a character sequence of [0…9] [A…Z] [a…z] [_].
  › The first character cannot be a digit.
  › There is no difference between small letters and capital letters.

› `<Filter>`:

  › The output of some commands can be restricted by entering a filter expression. Filtering does not occur line by line, but in blocks, depending on the command.

- A filter expression starts with the "@" symbol by itself and ends either at the end of the line or at a ";" (semicolon) to end the current command.
- A filter expression also consists of one or more search patterns, which are separated by blank spaces and preceded either by no operator (OR pattern), a "+" operator (AND pattern) or a "-" operator (NOT pattern).
- For the execution of the command, an information block is output exactly when at least one of the "OR" patterns, all "AND" patterns or none of the "NOT" patterns matches. Capitalization is ignored.
- For a search pattern to contain characters for structuring in the filter syntax (e.g., blank characters), then the entire search pattern can be enclosed in "". Alternatively, the symbol "\" can be placed before the special characters. If you want to search for a quotation mark (") or "\", another "\" symbol has to be placed in front of it.

Entering the start of the word, if it is unique, is sufficient.

Explanations for addressing, syntax and command input

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, the command `cd setup` can be shortened to `cd se`. The input `cd /s` is not valid, however, since it corresponds to both `cd /Setup` and `cd /Status`.
- The values in a table row can alternatively be addressed via the column name or the position number in curly brackets. The command `set ?` in the table shows the name, the possible input values and the position number for each column.
- Multiple values in a table row can be changed with **one** command, for example in the WLAN networks (`/Setup/WLAN/Network`):
  - `add Guest Guest 1234567890` creates a new network named Guest, SSID Guest, and key 1234567890.

    The order of the values must correspond to their order in the table. Values that should not be changed can be specified with a *.
  - `set Guest * 0987654321` changes the value Key in the network Guest. Using the * leaves the SSID unchanged.
  - `set Guest {Key} 1234567890` sets the value Key in the network Guest. Individual columns can be referenced by the column name in parentheses.
- Names that contain spaces must be enclosed within quotation marks (“”).

Command-specific help

- A command-specific help function is available for actions and commands (call the function with a question mark as the argument). For example, `show ?` displays the options available with the show command.

3 Feature descriptions

A selection of WLAN features is described in the following.

3.1 WLC layer-3 tunnel

Layer-3 tunneling involves the extended application of the CAPWAP protocol (control and provisioning of wireless access points) as used by WLAN controllers (WLC) to manage WLAN access points. It allows WLAN data to be fed into the LAN via a central WLAN controller by establishing a direct data tunnel between the WLAN controller and the access point. For configuration, one of the available WLC tunnel interfaces has to be set in the logical network profile of the WLC under **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)** > **Connect SSID to**. The data traffic from that SSID is now directed to the selected WLC tunnel interface of the WLC. The WLC tunnel interface can now be used for an ARF network or in the LAN bridge of the WLC.

Layer-3 tunneling is ideal for environments operating unmanaged switches or where no further VLAN configuration of the switches is possible. This allows data tunnels to be set up very quickly and easily without needing a VLAN infrastructure between the WLAN controller and access point to isolate the data traffic of individual SSIDs from one another. A VLAN infrastructure is only required at the transfer point between the WLAN controller and the local networks because data from the individual SSIDs is transported in a layer-3 tunnel between the access point and WLAN controller. Alternatively, the WLAN controller can use its router function to route data delivered via the tunnel to other IP networks or to the Internet.

To use this feature, the R&S®NC WLAN controller requires LCOS 10.42 RU3 or higher.

3.2 Band steering

The IEEE 802.11 standard contains virtually no criteria by which a WLAN client should select the access point for a connection. While there are, for example, general guidelines for the preference given to an access point with a higher RSSI value (i.e. the received signal strength), WLAN clients do not, in practice, adhere strictly to these definitions or the general guidelines. If both 2.4 GHz and 5 GHz are used to broadcast an SSID, there is normally no way of influencing the client as regards the preferred frequency band.

“Client steering” is based on the principle that many clients discover the available access points by means of an active scan. Active scanning here means that a client sends probe requests containing the network ID to which the client is to connect. Access points with this ID then send a test response, enabling the client to create a list of available access points. The vast majority of WLAN clients only connect to access points from which they have received a probe response, and this can be used to steer their selection process.

There are several, sometimes highly advanced, criteria for steering. One of these criteria relates to the wireless frequency ranges used for client communication. Modern dual-band WLAN clients are expected to prefer the 5 GHz frequency band over the now overcrowded 2.4 GHz band. Band

Steering is the term given to purposefully assigning a WLAN client to a particular frequency band or range.

The list of detected or “seen” clients contains all clients from which the access point has received a test request packet. In combination with the radio frequency on which the WLAN client sends the probe request, this list is one of the bases used by the access point to decide whether or not to respond to the request.

Other criteria depend on the reported client IDs and the configuration of the devices. It may be the case, for example, that fewer SSIDs are reported on the preferred frequency band than are on the one with the lower preference. Similarly, too low a transmit strength when SSIDs are reported can result in the client not receiving any probe responses at all on the preferred frequency band. For the latter scenario, it is important to ensure that the access point does not suppress probe responses on the less favored frequency band.

To configure the access point's band steering function with LANconfig, go to **Wireless LAN** > **Client management**.

3.3 Fast roaming

By operating authentication according to the IEEE 802.1X standard and key management according to the IEEE 802.11i standard, modern WLAN installations offer a high degree of security and confidentiality for the transmitted data. However, these standards require transmission of additional data packets during the connection negotiation as well as additional computing power on the client and server.

IEEE 802.11 originally required up to six data packets to establish a data connection between a WLAN client and an access point. The standard extension IEEE 802.11i improved on weak points of WEP encryption; however, depending on the authentication method, it substantially increased the length of the login process.

This extra time for the WLAN client to login to the access point is not a problem for non-time-critical applications. However, for smooth, loss-free roaming of a WLAN client from one access point to the next, a delay of more than 50 ms is not acceptable. Examples include Voice-over-IP (VoIP) or the application in real-time industrial environments. In this context, roaming means that the network connection passes from one access point to the other without interruption.

Methods such as pair-wise master key caching (PMK caching), pre-authentication, Opportunistic Key Caching (OKC) and the use of central WLAN controllers (WLC) for key management improve the time for the key negotiation between the WLAN client and access point during login. Despite this, the comparatively long time required for key negotiation between the WLAN client and the access point has still not been reduced to a viable extent.

Along with the improved encryption protocols, IEEE 802.11e makes it possible to reserve additional bandwidth with the access point. This allows the WLAN client to prevent interruptions, for example for VoIP connections at times of high network loads at the access point. For roaming from one access point to the next, the WLAN client must again reserve this additional bandwidth on the new access point. However, the additional management frames required for this considerably increase the login time.

The IEEE 802.11r standard provides a simplified authentication process for mobile WLAN clients to roam trouble-free from one access point to the next. The goal is to once again reduce the number of data packets for the login on the access point to the four to six packets known from IEEE 802.11.

Similar to Opportunistic Key Caching (OKC), a centralized key management (preferably by a WLC) supplies the access points connected to it with the credentials of the WLAN clients. In contrast to

OKC, the WLAN client performing fast roaming can detect whether the access point supports IEEE 802.11r

Access points managed by the WLC transmit the “mobility domain information element (MDIE)” to inform WLAN clients within range about, among other things, which “mobility group” the access point belongs to. Based on this information, the WLAN client detects whether it belongs to the same domain and can therefore authenticate without delay. This mobility domain is announced to a WLAN client the first time it authenticates at an access point.

The domain identifier and other special keys generated during the initial authentication and transmitted to all managed access points now reduce the stages of negotiation to the desired four to six steps when authenticating at a new access point.

To avoid futile and thus time-wasting login attempts with expired PMKs, IEEE 802.11r provides additional information about the validity periods of keys. In this manner, the client negotiates a new PMK while connected to the current access point. This is also valid on the access point that the WLAN client wants to connect to next.

Additionally, IEEE 802.11r uses “resource requests” to reserve additional bandwidth on the new access point, so that there is no need to cause added delay by transferring unnecessary data packets during the IEEE 802.11e authentication.

Older WLAN clients may have trouble establishing a connection to an SSID with enabled 802.11r. Therefore, it is advisable to use two SSIDs here: One SSID for older clients without 802.11r support and another SSID with enabled 802.11r for clients that support 802.11r.

Fast roaming is setup in LANconfig under **Wireless LAN** > **General** > **Encryption** > **WPA2/3 key management**.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Fast roaming by Inter Access Point Protocol (IAPP)

In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. When a client switches to another access point, the new access point sends a handover request to the former access point. The former access point then deletes the client from its station table. The handover request contains the client’s MAC address, so that devices in the LAN are informed about the new routing and can update their mapping table.

To enter the IAPP passphrase in LANconfig, navigate to **Wireless LAN** > **General** > **Encryption** > **PMK-IAPP secret**.

Please note that to use Fast Roaming by IAPP, it is necessary to select Fast Roaming in the encryption settings under WPA2 key management.

3.4 R&S®NC Enhanced Passphrase Security (LEPS)

R&S®NC Enhanced Passphrase Security (LEPS) allows a set of passphrases to be configured and assigned to individual users, groups or MAC addresses. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

This is useful for onboarding devices into the network. For example, a network operator “onboarding” multiple WLAN devices into different areas of the network does not want to configure each specific device; instead this should done by the users of the devices themselves. In this case, users are given a preshared key for the company WLAN for use with their own devices. LEPS is configured entirely on the infrastructure side, which assures full compatibility to third-party products.

The security issue presented by global passphrases is fundamentally remedied by LEPS. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should “get lost” or an employee with knowledge of their passphrase leaves the company, then only the passphrase of that user needs to be changed or deleted. All other passphrases remain valid and confidential.

Along with passphrases for users, **individual** passphrases consisting of any sequence of 8 to 63 ASCII characters can also be assigned to MAC addresses. Authentication at the access point is only possible with the correct combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS thus shuts out a potential attack on the ACL. If WPA2 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN, because knowledge of both the MAC address and the passphrase is required before encryption can be negotiated.

Compared to LEPS for users, the administrative overhead is slightly higher because the MAC address has to be entered for each device.

For technical reasons, LEPS is only compatible with WPA version WPA2.

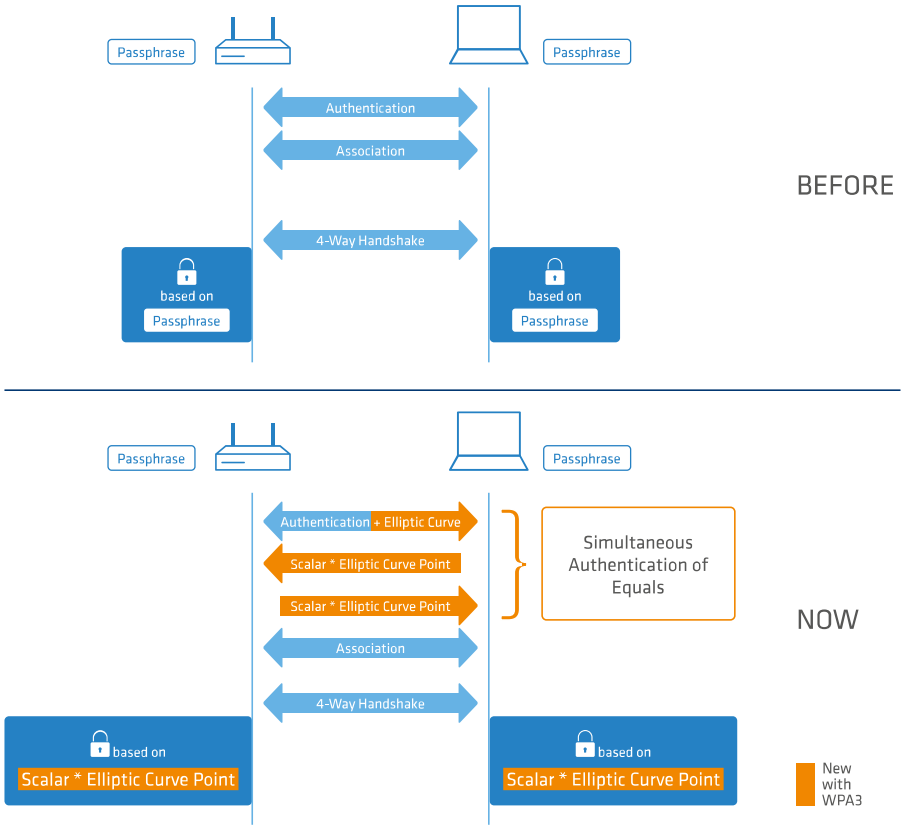
For technical reasons, LEPS is not compatible with Fast Roaming for user accounts that have a passphrase but no MAC address.

3.5 WPA3 (Wi-Fi Protected Access 3)

Compared to the predecessor standard WPA2 introduced by the Wi-Fi Alliance in 2004, the WPA3 standard introduced in 2018 offers improved security by combining various security methods. Like WPA2, WPA3 also exists in the versions WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) authentication method, which only requires a password for authentication but which prevents brute-force and dictionary attacks. Furthermore, for the first time this method offers forward secrecy, i.e. captured

WPA3-secured traffic cannot be decrypted subsequently after the attacker gains knowledge of the pre-shared key.



In addition, the WPA3-Enterprise uses the Commercial National Security Algorithm (CNSA) Suite B cryptography. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Both variants now require the use of protected management frames (PMF) according to IEEE 802.11w. PMF prevents attackers from computing the WLAN password from captured material gained by using fake management frames to force a disassociation and then eavesdropping the re-authentication.

3.5.1 WPA3-Personal

In the WLAN encryption settings under **Wireless LAN** > **WLAN networks** > **Encryption**, the WPA versions **WPA3** and **WPA2/3** are available for selection.

With **WPA3** selected, only WLAN clients that support WPA3-Personal will be able to login. This configuration enforces authentication with the Simultaneous Authentication of Equals (SAE). Similarly, this SSID enforces the use of PMF (Protected Management Frames as per IEEE 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

3.5.2 WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Rather, it set out policies to ensure greater consistency in the application of these protocols and to assure the desired level of security.

In the WLAN encryption settings under **Wireless LAN** > **WLAN networks** > **Encryption**, the WPA versions **WPA3** and **WPA2/3** are available for selection.

By selecting **WPA3**, only WLAN clients that support WPA3-Enterprise will be able to log in. This SSID enforces the use of PMF (Protected Management Frames as per IEEE 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

Suite B cryptography

In addition, the WPA3-Enterprise uses the Commercial National Security Algorithm (CNSA) Suite-B cryptography. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

Use of the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

The RADIUS server integrated in the LCOS supports the cipher suites mentioned here.

4 Configuring features with LANconfig

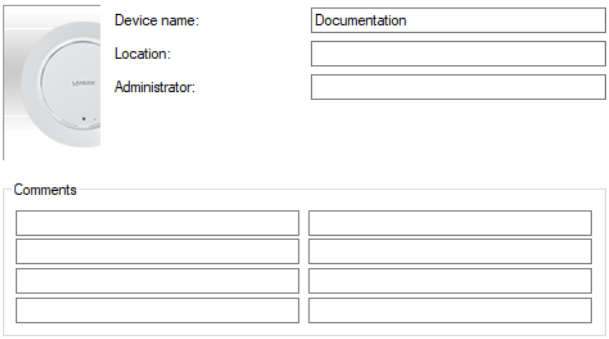
The following explains all of the options for adjusting settings with LANconfig. These depend on the device, so not all of the listed options are available with every device.

4.1 Management

The **Management** section contains general settings for the device.

4.1.1 General

The device settings described here are to be found under **Management** > **General**.



Name

Configure the device name here.

Location

Configure the device location here.

Administrator

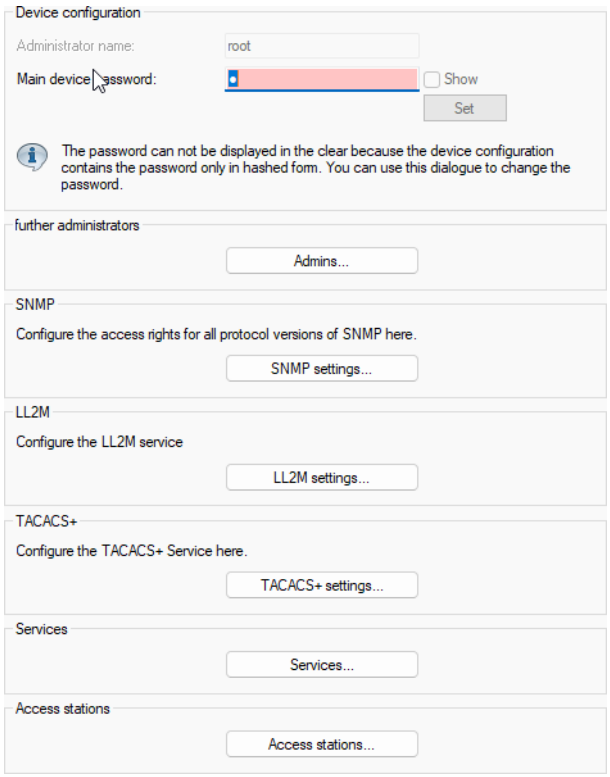
Here you configure the name of the device administrator.

Comments

Use the comment fields to enter any comments about the device configuration.

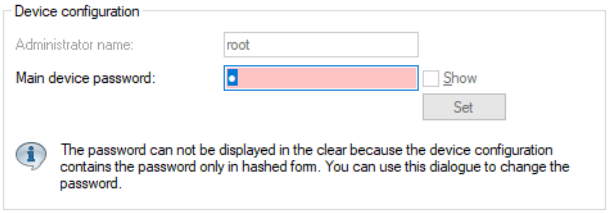
4.1.2 Admin

The settings for changing the main device password and SNMP can be found under **Management** > **Admin**.



4.1.2.1 Main device password

The settings for changing the main device password are located under **Management** > **Admin** > **Device configuration**.



Administrator name

Here you configure the login name of the device administrator. Depending on the device, this name may be fixed and will only be displayed here.

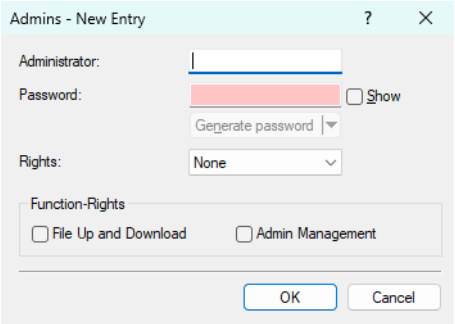
Main device password

Configure the main device password here. Depending on the device, this may be stored as a hash value and consequently cannot be displayed as plain text.

If you enter a new password, a field appears to repeat the entry of the changed password. Your input is not displayed, so this serves to verify your input. Alternatively, you can activate the option **Show**. Your input is then displayed in a legible form. We do not recommend this option if other individuals can view your screen while you type.

4.1.2.2 Additional Administrators

Not every configuration task requires an administrator with full permissions. As a root administrator, you can create administrators with restricted permissions. This means that the main device password does not have to be known to every administrator. Additional administrators are configured under **Management** > **Admin** > **Admins**.



Administrator

The name of the new administrator account.

Password

The password of the new administrator account.

Rights

Select one of the following access rights:

- **None:** The configuration cannot be read or written, but a CLI login for executing commands is possible.
- **Admin-RO:** The configuration can be read but not written.
- **Admin-RW:** The configuration can be read and written.

Function-Rights

Select from the following function rights:

- **File Up and Download:** This function right is required to transfer files, for example via SCP, such as the support information file.
- **Admin Management:** This function right is required to configure additional administrators on the device.

4.1.2.3 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) enables devices on a network to be monitored and configured from a central instance. Since the initial release of SNMPv1 in 1988, it has continued to evolve with the versions SNMPv2 and SNMPv3 to meet the needs of increasingly complex network infrastructures and the demands for user-friendliness, security and flexibility.

The protocol SNMP (simple network management protocol) meets the highest standards for convenient management and monitoring of a network. It allows for the early detection of problems and errors on a network and offers support in eliminating them. The simple network management protocol allows a central instance to monitor and configure the devices on a network from, and it regulates the communication between the monitored devices and the monitoring station. This means that parameters such as the status of the device, CPU utilization, the temperature of a device, its connection status, errors, and others can be monitored and analyzed, for example with LANmonitor. The administrator benefits from active support with network management and is helped to detect problems at an early stage. The latest SNMPv3 version of the protocol, in contrast

to the previous versions SNMPv1 and SNMPv2, now enables encrypted data communication between the network and its management system, which provides a crucial security factor. By offering different user accounts for authentication, the integrated user administration provides optimal control over access to the configurations. You have precise control over the rights to the different levels of access that administrators receive, and the network is optimally protected.

SNMP components

The typical SNMP architecture consists of three components:

SNMP manager

The SNMP manager sends SNMP requests to the SNMP agent and evaluates the SNMP responses from it. LANconfig and LANmonitor act as this type of SNMP manager. LCOS LX devices comply with the standards SNMPv1, SNMPv2, and SNMPv3, so it is possible to use an alternative SNMP administration and management software.

SNMP agent

The SNMP agent is a module that is active on the managed device. When it receives a request from the SNMP manager, it retrieves the requested status data from the MIB in the device and returns this information to the SNMP manager as an “SNMP response”. Depending on the configuration, an SNMP agent that detects certain changes of state in the managed device can independently act to send an “SNMP trap” to the SNMP manager. It is also possible to send a notification to the device administrator by means of a SYSLOG message or e-mail.

Managed device

The status of this device is stored in its Management Information Base (MIB). When requested by the SNMP agent, the device reads out this information and returns it to the SNMP agent.

By default, SNMP requests and SNMP responses are exchanged between the SNMP manager and SNMP agent by the User Datagram Protocol (UDP) on port 161. SNMP traps are transmitted with the UDP via port 162 by default.

SNMP versions

The differences between the various versions of SNMP can be summarized as follows:

SNMPv1

Version 1 was launched in 1988 and has long been regarded as the de facto standard for network management. In SNMPv1, the SNMP manager authenticates at the SNMP agent by means of a community string, which must be identical on both components. The security of this is very limited, as the community strings are transmitted in cleartext. The increase in demands for secure network communication necessitated a revision of version 1.

SNMPv2

After 1993, the main improvements in version 2 were to its user-friendliness. Numerous intermediate steps and the repeated rejection of concepts eventually led to the version SNMPv2c. This version allows large amounts of data to be requested via a `GetBulkRequest` command and also the communication between SNMP managers. However, the exchange of the community strings was still as cleartext as with version 1.

SNMPv3

From 1999, version 3 finally met the by then much-needed security requirements. Among other things, the communication was encrypted and the communication partners first had to authenticate and authorize themselves. Also, the structure of SNMP became more modular so that improvements, for example in encryption technologies, can be incorporated into SNMPv3, without having to completely redesign the standard.

LCOS LX supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

4.1.2.3.1 SNMPv3 basics

The SNMP protocol structure has changed significantly with version 3. SNMPv3 is now divided into a number of modules with clearly defined interfaces that communicate with one another. The three main elements in SNMPv3 are “Message Processing and Dispatch (MPD)”, “User-based Security Model (USM)” and “View-based Access Control Mechanism (VACM)”.

MPD

The MPD module is responsible for the processing and dispatch of inbound and outbound SNMP messages.

USM

The USM module manages security features that ensure the authentication of the users and the encryption and integrity of the data. SNMPv3 introduced the principle of the “security model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the “security model” accordingly.

VACM

VACM ensures that the sender of an SNMP request is entitled to receive the requested information. The associated access permissions are found in the following settings and parameters:

SNMPv3-Views

“SNMPv3-Views” collect together the content, status messages, and actions of the Management Information Base (MIB) that are permitted to receive or execute an SNMP request. These views can be single values, but also complete paths of the MIB. This content is specified by the OIDs of the MIB entries.

In this way, a successfully authenticated sender of an SNMP request only has access to that data specified in the applicable SNMPv3 views.

SNMPv3-Groups

“SNMPv3-Groups” collect users with the same permissions into a specific group.

Security-Levels

“Security levels” relate to the exchange of SNMP messages. The following levels can be selected:

NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

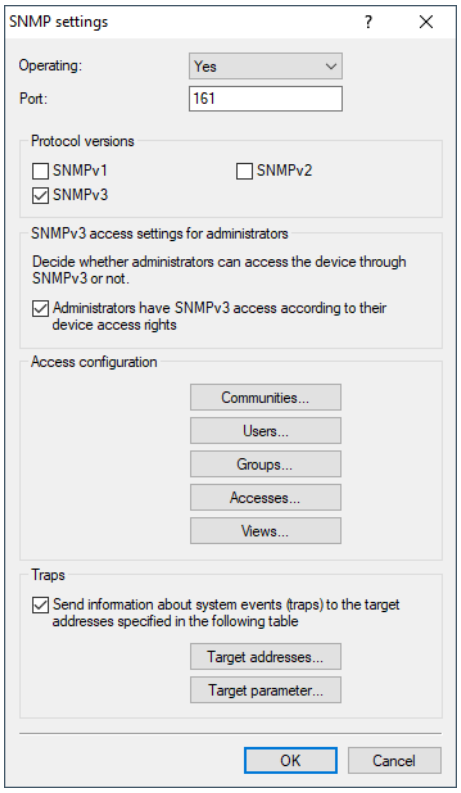
SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Context

“Context” is used to distinguish the various SNMP entities.

4.1.2.3.2 Configuring SNMP

The SNMP settings of the device can be found under **Management** > **Admin** > **SNMP** > **SNMP settings**.



Operation

Enable SNMP for the SNMP protocol versions specified below, which the device should support for SNMP requests and SNMP traps.

Port

If necessary, adjust the port used for SNMP. Default: 161

Protocol versions

SNMPv1

Enables SNMPv1.

SNMPv2

Enables SNMPv2c.

SNMPv3

Enables SNMPv3.

SNMPv3 access settings for administrators

Administrators have SNMPv3 access according to their access rights

Enable this option if registered administrators, including the root user, should also have access via SNMPv3.

Access configuration

SNMP communities

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a “community”. Authentication is optionally handled

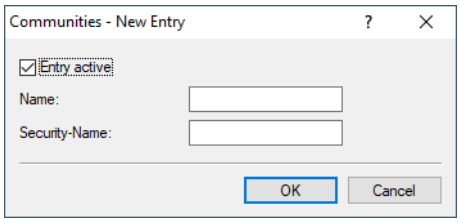
- by the `public` community (unlimited SNMP read access),
- by a master password (limited SNMP read access),
- or a combination of user name and password, separated by a colon (limited SNMP read access)

.

A community collects certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community `public`. Because this represents a potential security risk, especially with external access, LANconfig gives you the option of defining your own communities.

This configuration is relevant for the SNMP versions v1 and v2c only.



Entry active

Activates or deactivates this SNMP community.

Name

Enter a descriptive name for this SNMP community.

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

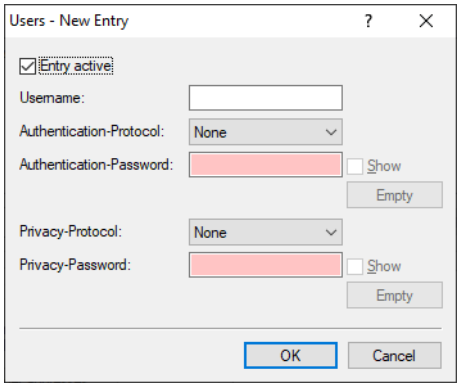
The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the `public` community in the list of the SNMP communities. This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community `public` has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

Users

Individual users can be granted access to the device in addition to the administrators registered on it. Here you configure the authentication and encryption settings for these users when operating SNMPv3.



Entry active

Activates or deactivates this user.

User name

Enter a descriptive name for this user.

Authentication

Specify the method that the user is required to use to authenticate at the SNMP agent. The following options are available:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA- 224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA- 256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA- 384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA- 512 (hash length 512 bits).

Authentication password

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

Encryption

Specify which encryption method is used for encrypted communication with the user. The following options are available:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits)

AES192

Encryption is performed with AES192 (key length 192 bits)

AES256

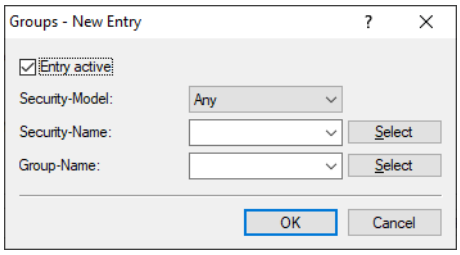
Encryption is performed with AES256 (key length 256 bits)

Privacy password

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

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.



Entry active

Activates or deactivates this group.

Security model

SNMPv3 introduced the principle of the “security model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the “security model” accordingly. Select one of the following entries accordingly:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv3_USM

Data is transmitted by SNMPv3. Security levels for the user’s authentication and communication are possible, and these levels are activated with the **access rights**.

Security-Name

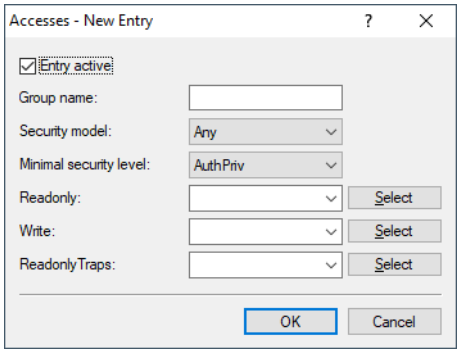
Here you select a security name you assigned to an SNMP community.

Group name

Here you select a group that you want to define under **Access rights**.

Access rights

This table brings together the different configurations for access rights, security models, and views.



Entry active

Activates or deactivates this entry.

Group name

Enter a descriptive name for this group.

Security model

Activate the appropriate security model here.

Minimal security level

Specify the minimum security level for access and data transfer.

NoAuthNoPriv (No authentication/No privacy)

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv (Authentication/No privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

AuthPriv (Authentication and privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

Read

Set the view of the MIB entries for which this group is to receive read rights. Available values are those defined under **Views**. Previously defined views are “Full Access”. “LANmonitor Access”. “Setup Access” and “Status Access”.

Write

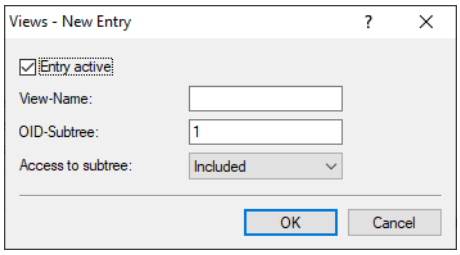
Set the view of the MIB entries for which this group is to receive write rights. Available values are those defined under **Views**. Previously defined views are “Full Access”. “LANmonitor Access”. “Setup Access” and “Status Access”.

Read-only traps

Set the view of the MIB entries for which this group is to receive read rights for traps. Available values are those defined under **Views**. Previously defined views are “Full Access”. “LANmonitor Access”. “Setup Access” and “Status Access”.

Views

Here you collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with the corresponding access rights.



Entry active

Activates or deactivates this view.

Name

Enter a descriptive name for this view.

OID subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in or excluded from this view.

The OIDs can be found in the device MIB, which you can download from *Download-Bereich*.

Access to subtree

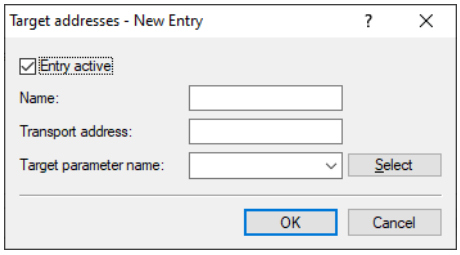
Here you decide whether the specified OID subtrees are “added” or “removed” from the view.

Traps

If you enable the option **Send information about system events (traps) to the target addresses specified in the following table**, the recipients configured under **Target addresses** and **Target parameters** will receive the corresponding information.

Target addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.



Entry active

Activates or deactivates this entry.

Name

Give the entry a descriptive name here.

Transport address

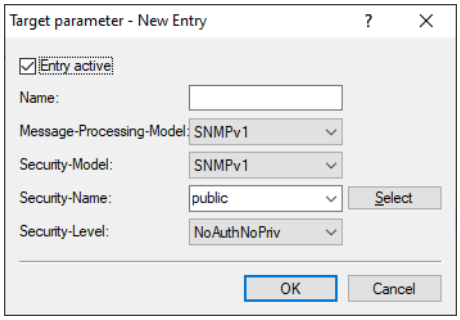
Configure the address of the recipient here. This address describes the IP address and port number of a recipient of an SNMP trap and is specified in the syntax “<IP address> : <Port>” (e.g. 128.1.2.3:162). UDP port 162 is used for SNMP traps.

Target parameter name

Here you select the desired entry from the list of recipient parameters.

Target parameter name

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.



Entry active

Activates or deactivates this entry.

Name

Give the entry a descriptive name here.

Message processing model

Here you specify the protocol for which the SNMP agent structures the message.

Security model

SNMPv3 introduced the principle of the “Security Model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to allow for the versions SNMPv2c or even SNMPv1, and to select these accordingly. Select one of the following entries accordingly:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv3_USM

Data is transmitted by SNMPv3. This can only be selected together with SNMP users. The effective possible security level depends on the user's chosen authentication and encryption methods.

Security-Name

Here you select a security name you assigned to an SNMP community.

Security level

Set the security level that applies for the recipient to receive the SNMP trap.

NoAuthNoPriv (No authentication/No privacy)

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv (Authentication/No privacy)

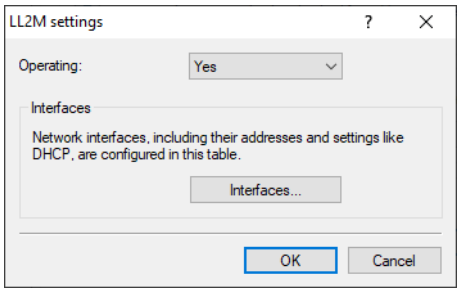
Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

AuthPriv (Authentication and privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

4.1.2.4 LL2M

The LL2M settings of the device can be found under **Management** > **Admin** > **LL2M** > **LL2M settings**.



Operating

A basic pre-requisite for all methods device configuration is for an IP connection to exist between the configuration computer and the device. No matter whether you use LANconfig, WEBconfig or SSH; it is impossible to send any configuration commands to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. The only option in this case is to access the device via the serial configuration interface, which however is not available on all devices, or to reset the device to its factory settings. However, both options require physical access to the device—this may not always be the case for the concealed installation of access points and can represent considerable overhead for larger-scale installations.

The **R&S®NC Layer 2 Management Protocol (LL2M)** is used to enable configuration access to a device even without an IP connection. All this protocol requires is a connection

on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server, which then responds to the requests or runs the commands. Both the LL2M client and the LL2M server are integrated in LCOS LX. The LL2M client commands are executed via the command line or WEBconfig.

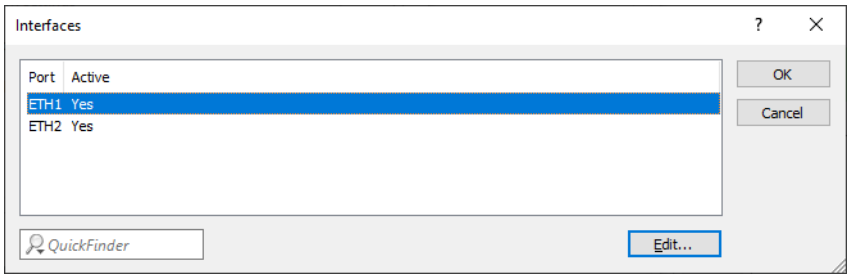
An encrypted tunnel is set up for every LL2M command to protect the transmitted log-in information. To use the integrated LL2M client, start a terminal session on a device that has local access to the LL2M server via the available physical medium (LAN, WLAN). In this CLI session you can use the following commands to contact the LL2M server: `LL2Mdetect` and `LL2Mexec`. See *Command-line interface — command summary* on page 10

Enable LL2M here.

Access points of type LANCOM LW-500 can only be discovered and configured via LL2M if they receive LL2M packets that contain a VLAN tag which is included in the access point‘s configuration (WLAN SSID configuration or management VLAN configuration).

Interfaces

This item is used to specify the interfaces or Ethernet ports where the LL2M server can be reached. The presetting provides accessibility on all Ethernet ports.



4.1.2.5 TACACS+

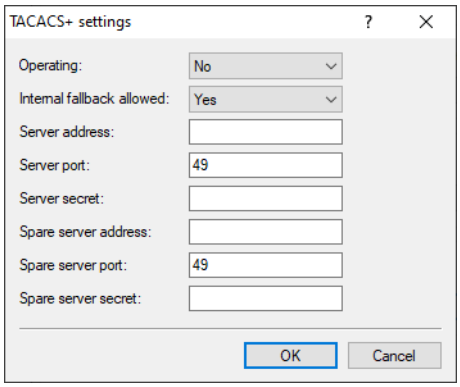
Configure authentication, authorization, and accounting (AAA) here using the TACACS+ protocol.

If this feature is active, admin logins are checked against the TACACS+ server and displayed and changed configuration items are transferred to the TACACS+ server for approval and/or logging.

The configuration points are transferred in OID representation.

When TACACS+ operation is active, the WEBconfig of the device is switched off.

The TACACS+ settings of the device can be found under **Management** > **Admin** > **TACACS+** > **TACACS+ settings**.



Operating

Switches the use of TACACS+ on or off.

Internal fallback allowed

If this option is activated, a login with local user data can be carried out if the TACACS+ server is not available.

Server address

The IP address of the primary TACACS+ server.

Server port

The port of the primary TACACS+ server.

Server secret

The key used for communication with the primary TACACS+ server.

Spare server address

The IP address of the backup TACACS+ server.

Spare server port

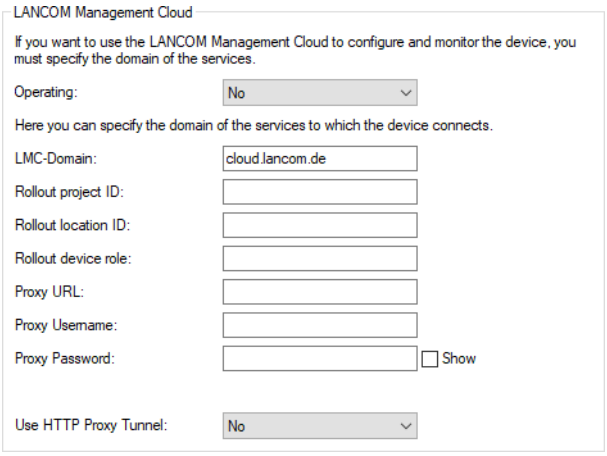
The port of the backup TACACS+ server.

Spare server secret

The key used for communication with the backup TACACS+ server.

4.1.3 LMC

Settings that relate to the configuration and monitoring of your device via the R&S®LANCOM Management Cloud (LMC) are located under **Management** > **LMC**.



Operation

Specify whether the device should be managed via the LMC.

No

The device does not connect to the LMC.

Yes

The LMC manages the device.

LMC domain

Enter the domain name for the LMC here. By default, the domain is set to the Public LMC for the first connection. If you wish to manage your device with your own Management Cloud (“Private Cloud” or “on-premises installation”), please enter your LMC domain.

Rollout project ID

Enter the project ID of this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

Rollout location ID

Enter the location of this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

Rollout device role

Enter the role assigned to this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

4.1.4 Extended

Here you will find the settings for the LED functionality, the option to send the syslog to external servers and settings for SSH.

4.1.4.1 LED

The settings for the LED functions are located here. These are located under **Management** > **Extended**.



For devices that require PoE 802.3bt for full functionality (e.g. activation of all WLAN streams), a permanently lit yellow power LED indicates that there is insufficient power supply.

LED-Mode

Choose between the different LED modes.

On

The LED(s) of the device are permanently in operation and signal the operating state.

Off

The LED(s) of the device are switched off immediately after starting.

Timed off

The LED(s) of the device are switched off after the configured time.

Refer to the Quick Reference Guide for device-specific details about LED signaling.

LED off seconds

Set a time in seconds after the device starts, after which the LED(s) of the device are switched off if the **LED mode** is set to Timed-Off.

4.1.4.2 PoE Passthrough

This item contains the PoE Passthrough settings. These are located under **Management** > **Extended**.



PoE Passthrough

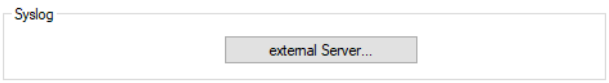
For models with the PoE Passthrough feature, supplying the access point with PoE 802.3bt (60W) allows a further PoE device (PD) to be connected to the second Ethernet port ETH2, and this in turn can be fed with a maximum of 30W.

This item switches the PoE Passthrough feature on and off. In the factory default settings it is deactivated. LANmonitor and WEBconfig provide additional status information.

4.1.4.3 Syslog

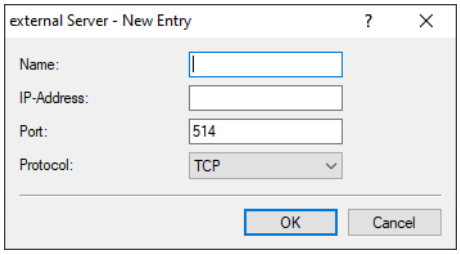
For diagnostic purposes, the syslog of a LCOS LX-based device can be sent to an external syslog server.

The settings for this can be found under **Management** > **Extended** > **Syslog**.



Configure one or more syslog servers in the **External Server** table. Messages can be sent via TCP or UDP.

Note that syslog messages are unencrypted and may contain sensitive information about your network. For this reason they should only be transmitted for diagnostic purposes over a secure network.



Name

Name of the external syslog server.

IP address

IP address of the external syslog server.

Port

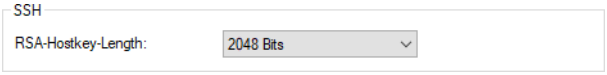
Port of the external syslog server.

Protocol

Protocol (TCP/UDP) used to communicate with the external syslog server.

4.1.4.4 SSH

Under **Management** > **Extended** you will find the settings for the SSH functionality.



RSA-Hostkey-Length

The length of the SSH host key can be selected between 2048 bits and 4096 bits. After changing the setting, the hostkey is regenerated immediately.

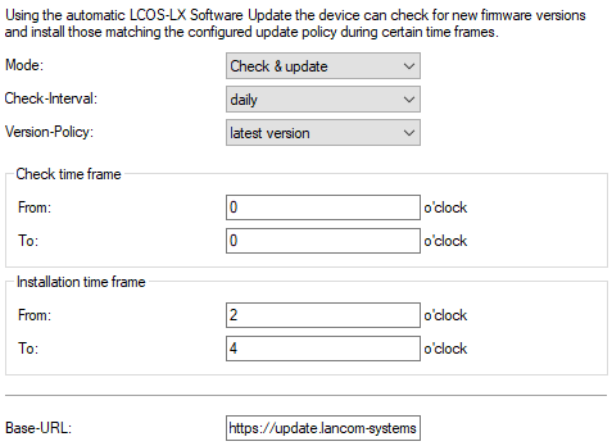
4.1.5 Software update

The R&S®NC Auto Updater allows the automatic updating of on-site R&S®NC devices without further user intervention. R&S®NC devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The R&S®NC Auto Updater contacts the R&S®NC update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the R&S®NC device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current

R&S®NC devices are signed. The R&S®NC Auto Updater validates this signature before uploading any firmware.

The configuration for the R&S®NC Auto Updater in LANconfig is located under **Management** > **Software update**.



Mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security patches only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest version w/o REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 REL.

Check time frame

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

Installation time frame

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Base URL

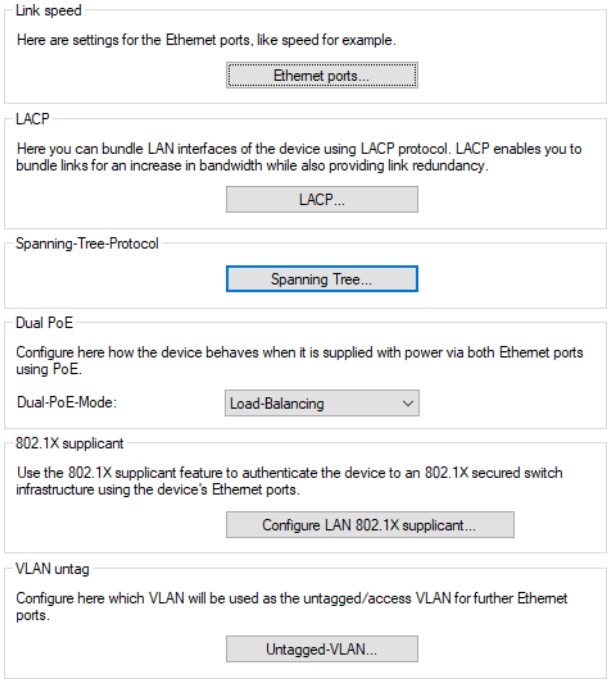
Specifies the URL of the server that provides the latest firmware versions.

4.2 Interfaces

The section **Interfaces** contains the settings for the device's interfaces.

4.2.1 Port settings

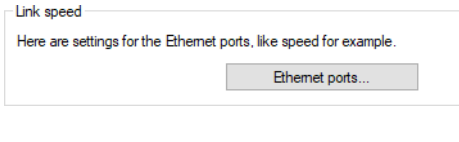
The settings for configuring the Ethernet ports of the device are located under **Interfaces** > **Port config**.

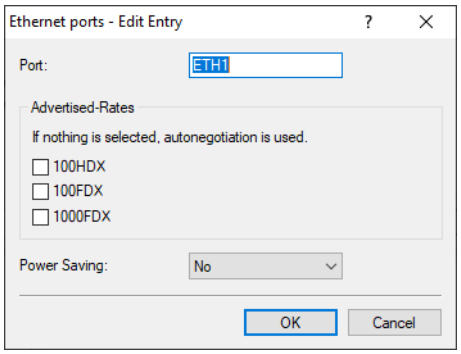


4.2.1.1 Link speeds

Settings for the Ethernet interfaces can be found here, such as for the speed or to activate Energy Efficient Ethernet/IEEE 802.3az.

LANconfig: **Interfaces** > **Port config** > **Link speed** > **Ethernet ports**





Port

Configure the Ethernet port that these settings apply to.

Advertised rates

Configure the rates advertised for this Ethernet port here. With no value selected, auto-negotiation is used.

Power-Saving

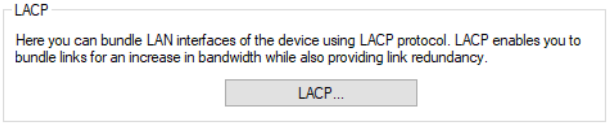
Use this parameter to enable or disable Energy Efficient Ethernet/IEEE 802.3az for this Ethernet port.

4.2.1.2 Link Aggregation (LACP)

Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle LAN ports into a virtual link. Physical connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

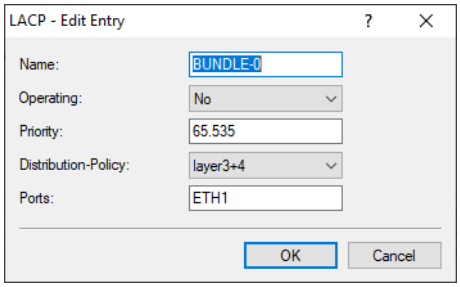
Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

LANconfig: **Interfaces** > **Port config** > **Link Aggregation**



4.2.1.2.1 LACP (Link Aggregation Control Protocol)

The **LACP** menu is used to configure the Link Aggregation Control Protocol.



Name

This is the logical interface used to bundle the selected physical interfaces.

Operating

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together into one common logical bundled interface. In the disabled state the interfaces that are selected in the corresponding table still operate as individual interfaces.

Priority

Enter the LACP system priority. The default value is 65,535.

Distribution-Policy

There are a number of options for distributing the network packets to the various bundled interfaces. The following characteristics are used for distribution:

layer2

MAC addresses

layer2+3

A combination of MAC addresses and IP addresses

layer3+4

IP addresses and TCP/UDP ports

encap2+3

Like layer2+3. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

encap3+4

Like layer3+4. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

Ports

Use this parameter to select the physical interfaces as a comma-separated list that the device bundles via LACP. Default: ETH1,ETH2

4.2.1.3 Spanning Tree Protocol

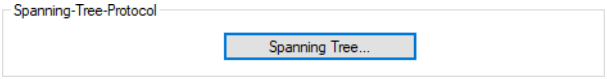
In networks with multiple switches and bridges, there can be multiple physical connections between two connected network participants. These redundant data paths are desirable, as they provide alternative routes to the destination if individual network segments fail. On the other hand, these multiple connections can lead to undesirable loops or duplicate frame reception. Both effects disrupt the smooth flow of data in the network.

In particular, when using R&S®NC LX-7500 access points for hitless failover, the use of the (Rapid) Spanning Tree Protocol ((R)STP) is essential to ensure redundancy not only in power supply but also in data transmission and to prevent the formation of a loop.

Alternatively, LACP can also be used in conjunction with hitless failover. Depending on the access point model, link speed and switching speed should be considered.

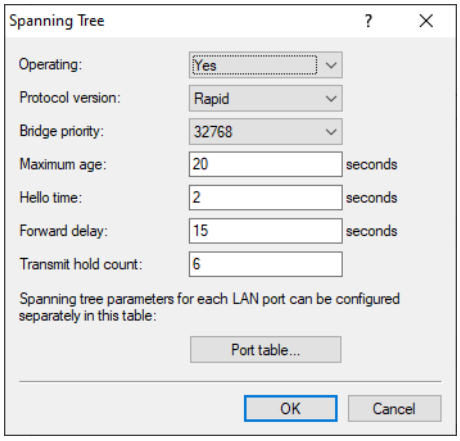
By default, RSTP is enabled on the R&S®NC LX-7500 to allow out-of-the-box operation with both Ethernet connections. In general, the Spanning Tree Protocol is supported by all access points with at least two Ethernet ports.

LANconfig: **Interfaces** > **Port Config** > **Spanning Tree Protocol**



4.2.1.3.1 Configuring the Spanning Tree Protocol

Use **Spanning Tree** to configure the Spanning Tree Protocol.



Operating

When Spanning Tree is disabled, a device does not send Spanning Tree packets and forwards any received Spanning Tree packets instead of processing them itself.

Protocol version

Classic

Uses the classic STP procedures for determining network topology.

Rapid

Uses the RSTP procedures for determining network topology.

RSTP is compatible with STP. If components in the network only support classic STP, STP procedures will be used even when RSTP is enabled.

Bridge priority

Sets the priority of the bridge in the LAN. This can influence which bridge is preferred as the root bridge by the Spanning Tree Protocol.

For compatibility with RSTP, this value should only be changed in increments of 4096, as RSTP uses the lower 12 bits of this 16-bit value for other purposes.

Maximum age

This value determines the time (in seconds) after which a bridge discards messages received via Spanning Tree as “stale”. This parameter defines how quickly the Spanning Tree algorithm responds to changes, e.g., due to bridge failures.

Modifying this time value is recommended only with a thorough understanding of the Spanning Tree Protocol. Adjustments may be useful to optimize response times to topology changes or to ensure stable operation in networks with many “bridge hops”.

Hello time

This parameter (in seconds) specifies the intervals at which a device selected as the root bridge sends Spanning Tree information to the LAN.

Modifying this time value is recommended only with a thorough understanding of the Spanning Tree Protocol. Adjustments may be useful to optimize response times to topology changes or to ensure stable operation in networks with many “bridge hops”.

Forward delay

This time (in seconds) specifies the minimum time that must pass before a Spanning Tree port is allowed to change state (Listening, Learning, Forwarding).

When using RSTP, the forwarding delay often has no effect, as RSTP has built-in mechanisms to trigger a fast transition to the forwarding state.

Modifying this time value is recommended only with a thorough understanding of the Spanning Tree Protocol. Adjustments may be useful to optimize response times to topology changes or to ensure stable operation in networks with many “bridge hops”.

Transmit hold count

Number of BPDUs that can be sent with RSTP before a one-second pause is enforced.

When using classic STP, the transmit delay has no effect.

Port table

The following values can be configured separately in the port table for all available ports (LAN, Wireless LAN, point-to-point links).

Priority

Sets the priority of the port. If there are multiple possible network paths with the same path cost, the priority determines which port is used. If the priorities are equal, the port that appears higher in the list is selected.

For compatibility with RSTP, this value should only be changed in increments of 16, as RSTP uses only the upper 4 bits of this 16-bit value.

Edge-Port

Marks the port as an edge port, to which no additional bridge is connected, only end devices like workstations or servers. Edge ports immediately switch to the forwarding state.

Edge ports are still monitored by RSTP. If BPDUs are detected on such a port, the port loses its status as an edge port.

Path-Cost-Override

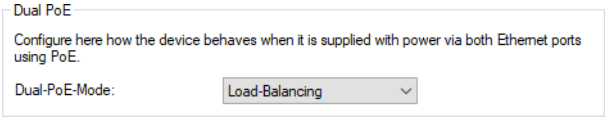
This parameter controls the priority of equivalent paths. The value set here is used in place of the calculated path cost for selection. The default value of 0 disables path cost override.

4.2.1.4 Dual PoE

Set the operating mode of the access point if it supports Dual PoE. With Dual PoE, both Ethernet ports can be used as PoE input.

The LANCOM LX-7500 access point supports Dual PoE—both Ethernet ports can be used as PoE input. In its factory settings, the LX-7500 is preconfigured for load balancing.

LANconfig: **Interfaces** > **Port config** > **Dual PoE** > **Dual-PoE Mode**



Hitless Failover

Allows uninterrupted operation of the access point if the PoE supply fails on one of the two Ethernet ports. The access point will not restart. This mode requires that the same PoE power is provided on both Ethernet ports.

In the case of the LX-7500, IEEE 802.3bt (Class 6 / 51W) is required for full operation.

Load Balancing

The access point draws power simultaneously via PoE from both Ethernet ports. Usually, the power drawn from both ports is similar, but ultimately this is influenced by the applied voltage and is therefore dependent on the specific circumstances.

This enables full operation of the R&S®NC LX-7500 with 2x IEEE 802.3at (Class 4 / 25.5W).

Monitoring on the CLI

You can view the settings or the current status via the CLI under **Status** > **Hardware-Info** > **Power** > **Failover-Status** (1.47.42.10). The following statuses are possible:

Disabled

The access point is not configured for Hitless Failover, but for Load Balancing.

Ready

The access point is configured for Hitless Failover, and PoE is provided through both ports. The failover event has not occurred.

Engaged

The access point is configured for Hitless Failover, but one of the ports has lost its PoE supply. The failover event has occurred.

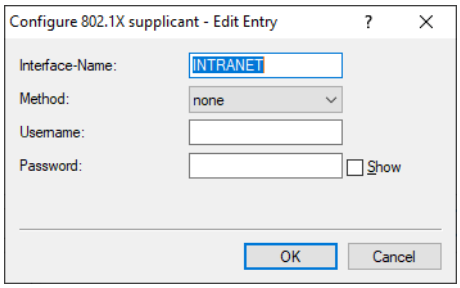
4.2.1.5 802.1X supplicant

These are the settings for the 802.1X supplicant functionality, which authenticates the device towards the LAN at a switch infrastructure secured by 802.1X. These are located under **Interfaces** > **Port config** > **802.1X supplicant**.



4.2.1.5.1 Configuring the 802.1X supplicant

You configure the 802.1X supplicant functionality under **Interfaces** > **Port config** > **802.1X supplicant** > **Configure 802.1X supplicant**.



Interface name

The name of the LAN interface. Currently there is only the interface INTRANET, and this cannot be changed.

Method

The EAP method used to authenticate at the 802.1X infrastructure.

User name

The user name to use to authenticate at the 802.1X infrastructure.

Password

The password to use to authenticate at the 802.1X infrastructure.

Support for authentication by means of client certificates will follow in a future LCOS LX version.

4.2.2 Layer-3 Ethernet tunnel with L2TPv3

LCOS LX supports the Layer 2 Tunneling Protocol (L2TP) in version 3. With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers, and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

L2TP uses two types of data:

Control data

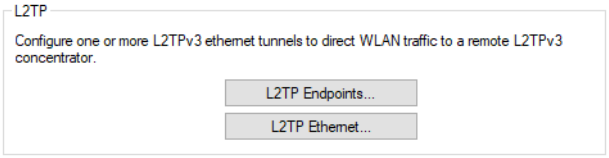
The control data are used to establish, maintain and tear down the tunnel connections. The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

Payload data

The payload data are encapsulated in Ethernet frames, which are exchanged between the LAC and the LNS via the tunnel. In contrast to the control data, payload data contains no data flow control. Thus there is no guarantee that the sender and receiver are exchanging data correctly.

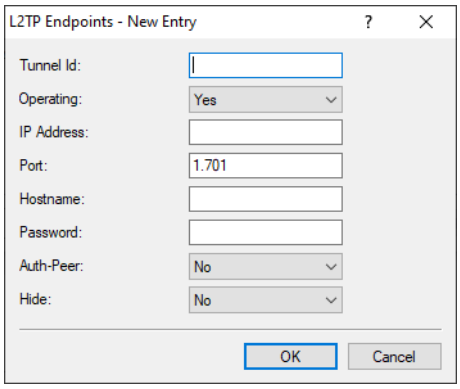
Unlike PPTP, which transfers control and payload data via different protocols (TCP and GRE), L2TP only uses UDP for both data types. You also have the option to operate multiple logical payload-data channels on each control-data channel.

LANconfig: **Interfaces** > **L2TP**



4.2.2.1 L2TP Endpoints

Use **L2TP Endpoints** to configure the L2TP endpoints for the L2TPv3 tunnels. This configures the tunnel so that the control data makes an L2TP tunnel into a tunnel endpoint.



Tunnel ID

The name of the tunnel endpoint. For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Operating

This L2TP endpoint is enabled or disabled.

IP Address

The IP address of the tunnel endpoint.

Port

UDP port to be used. Default: 1701

Hostname

User name for the authentication For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Password

The password for the authentication This is also used to hide the tunnel negotiations, if the function is activated.

Auth-Peer

Specifies whether the remote station should be authenticated.

Hide

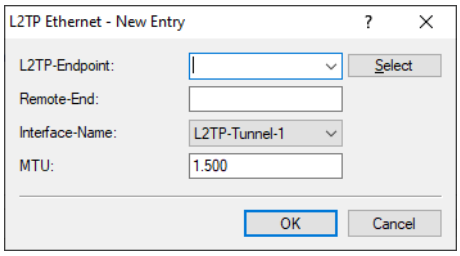
Specifies whether tunnel negotiations should be hidden by using the specified password.

Then connect a configured WLAN network to the virtual L2TP Ethernet interface.

To do this, go to **Wireless-LAN** > **WLAN-Networks** > **Network** and, for the desired entry, set the **Bridge** to the virtual L2TP Ethernet interface you just configured.

4.2.2.2 L2TP-Ethernet

The item **L2TP Ethernet** is used to configure the L2TPv3 tunnel between a WLAN network and an L2TP endpoint.



L2TP Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint.

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

Interface-Name

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

MTU

This setting adjusts the MTU of an L2TP Ethernet tunnel to the specified value, e.g. when connecting the tunnel across networks with smaller MTUs. Possible values: 68-1500

4.2.3 Multicast Snooping

All devices with WLAN interfaces have a “LAN bridge” that transfers data between the Ethernet ports and the WLAN interfaces. The LAN bridge works like a switch in many respects. The central task of a switch is to forward packets only to the port to which the receiver is connected. To do this, the switch automatically forms a table from the incoming data packets in which the sender MAC addresses are assigned to the ports.

If a destination address of an incoming packet is found in this table, the switch can forward the packet specifically to the correct port. If the destination address is not found, the switch forwards the packet to all ports. This means that a switch can only forward a packet specifically if the destination address has already been received by it once as the sender address of a packet via a specific port. However, broadcast or multicast packets can never be entered as the sender address in a packet, which is why these packets are always “flooded” to all ports.

While this behavior is the correct action for broadcasts, since broadcasts should eventually reach all possible recipients, it is not necessarily the desired solution for multicasts. Multicasts are usually aimed at a specific group of recipients on a network, not all of them.

For example, video streams are often multicast, but not all stations on the network should receive a particular stream.

Various applications in the medical field use multicasts to transmit data to specific terminals that should not be viewed at all stations.

With a LAN bridge in the device, there will therefore also be ports to which no single receiver of the multicast is connected. The “unnecessary” sending of multicasts on ports without receivers is not a mistake, but it leads to performance problems, especially in WLAN networks. There, the unnecessary sending of multicasts can lead to a significant restriction of the available bandwidth, since multicasts in the WLAN—just like broadcasts—are sent at the lowest possible transmission rate so that they can be received by every WLAN subscriber.

With the Internet Group Management Protocol (IGMP) for IPv4 as well as Multicast Listener Discovery (MLD) for IPv6, the TCP/IP protocol family provides a protocol with which the network stations can inform the router to which they are connected of their interest in certain multicasts. To do this, the stations register with the routers for specific multicast groups from which you want to obtain the corresponding packets (multicast registration). IGMP uses special messages to register (join messages) and deregister (leave messages) for this purpose.

Multicast snooping makes use of these messages to decide to which port (i.e., also to which WLAN SSID) multicasts must be sent.

LANconfig: **Interfaces** > **Multicast Snooping**



Operating

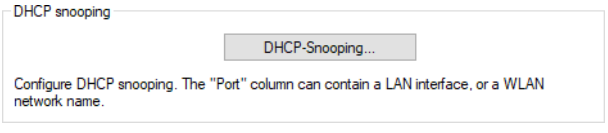
Turn multicast snooping on or off.

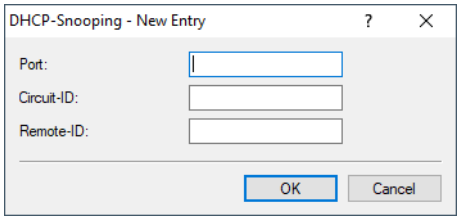
In addition, optional conversion of multicast data streams to unicast is possible. After activation of the feature, multicast data streams that are transmitted via WLAN interfaces are converted into individual unicast data streams for each client on the MAC layer or WLAN layer. The packets are duplicated for each client, but since they are now unicasts, they can be transmitted at the highest possible data rate for this client. Even though the packets are now duplicated, in most scenarios, the much faster transmission consumes much less airtime, which is then available for other transmissions. See *Multicast-to-Unicast* on page 62.

4.2.4 DHCP Snooping

The access point can add the Circuit ID and/or Remote ID to relayed DHCP packets. The DHCP server can make decisions based on this information, such as assigning specific IP addresses.

LANconfig: **Interfaces** > **DHCP Snooping**





Port

Here you can configure the WLAN network name or a LAN port (depending on the device model ETHx or LANx) on which DHCP requests should be supplemented.

Circuit-ID

The Circuit ID can be configured here using these placeholders:

- %i: Inserts the name of the interface where the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

Remote-ID

Here you can configure the Remote ID using these placeholders:

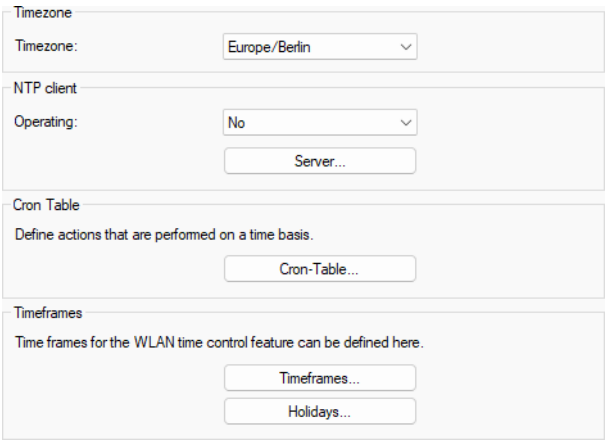
- %i: Inserts the name of the interface through which the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

4.3 Date/Time

The section **Date/Time** contains the corresponding device settings.

4.3.1 Configuration

The device settings date and time are to be found under **Date/Time** > **Configuration**.



Timezone

Set the correct time zone.

NTP client

Using the Network Time Protocol (NTP), the device can read the current time from a public time server on the Internet (NTP server with an “open access” policy such as the

Physikalisch-Technischen Bundesanstalt in Germany). R&S®NC routers also work as NTP servers, so not every network device needs to access an external NTP server.

Operating

Yes

The NTP server set under **Server** is used to set the date and time.

No

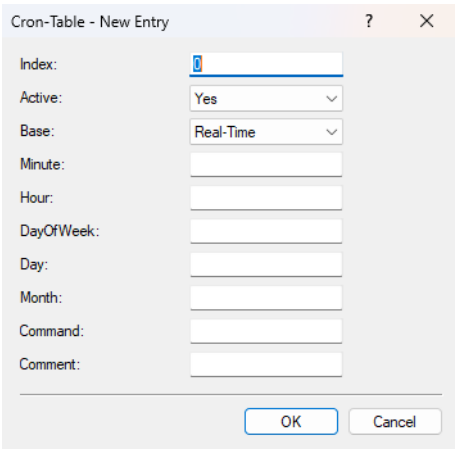
Do not use an NTP server.

Server

Select from the default NTP servers here or enter the address of the desired NTP server.

4.3.1.1 Time Automation via Cron Job

This feature enables the device to execute specific commands at specific, user-defined times. The functionality corresponds to the Cron service known from UNIX. Any command-line function can be executed. This means that all features can be controlled based on a schedule.



The function of the individual fields largely corresponds to the Cron job configuration known from Linux/Unix.

Index

Used to sort multiple Cron jobs.

Active

Determines whether the job is executed.

Base

The time base determines whether LCOS LX executes the command based on the device's real time or system uptime, that is, the time elapsed since the device was started.

Minute

The command is executed when the minute specified here is reached.

Hour

The command is executed when the hour specified here is reached.

DayOfWeek

The command is executed on the days of the week specified here using numbers. The digits representing the days of the week are separated by spaces. 0 represents Sunday, 1 represents Monday, …, and 6 represents Saturday.

Day

The command is executed on the days of the month specified here (from 1 to 31).

Month

The command is executed in the months specified here (from 1 to 12).

Command

The CLI command to be executed.

Comment

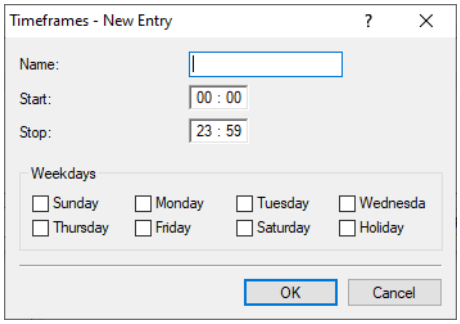
A free-text field for entering any comment.

4.3.1.2 Timeframes

Timeframes are used to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different timeframes. Add the time frame to the logical WLAN settings for it to be used with the corresponding SSID.

As an example, a number of timeframes have already been set up here to illustrate a configuration for a school day. There are two timeframes with the same name “Lessons” – but with different start and stop times in order to allow a 45-minute break between these two timeframes. This is defined in the time frame “Break”. Timeframes can be restricted to certain days of the week. Holidays are also taken into account as long as they are entered in the *Holidays table*. Summertime/wintertime is also observed based on the time zone setting.

Predefined timeframes are ALWAYS and NEVER. You can configure additional timeframes in LANconfig under **Date/Time** > **Configuration** > **Timeframes**. This section also allows you to specify public holidays for the timeframes.



Name

Enter the name of the time frame so that it can be referenced from the WLAN SSID. Several entries with the same name result in a common profile.

Start

The start time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile becomes valid.

Stop

The stop time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile ceases to be valid.

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

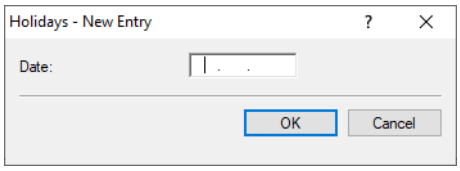
Here you select the weekday on which the timeframe is to be valid.

Possible values:

› Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

You can form a time schedule with the same name but with different times extending over several rows.

Holidays

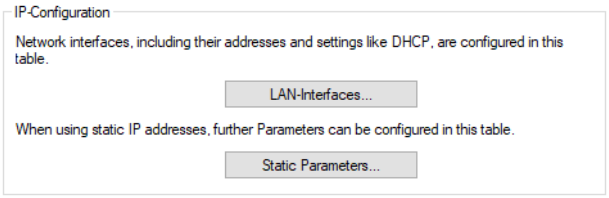


Enter the public holidays to be observed in the time frame.

The year 0 stands for any year.

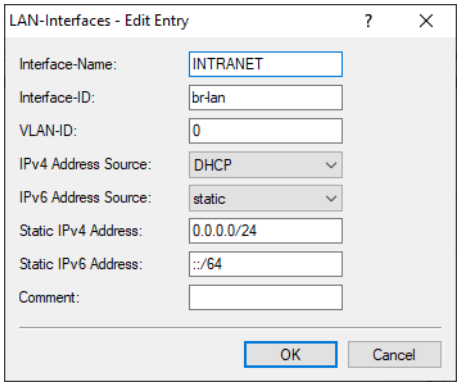
4.4 IP configuration

The settings for the IP configuration of your device are located under **IP Configuration** > **Configuration**.



4.4.1 LAN interfaces

Under **IP Configuration** > **Configuration** > **LAN interfaces** you can modify the basic configuration relating to the device's own IP settings and network access.



Interface name

Set a meaningful name for the interface here. This name is used to reference the interface configuration from other parts of the configuration.

Interface-ID

The internal identifier for the interface.

VLAN ID

Here you specify a VLAN ID for which the interface should be active and accessible. The default value “0” means that no VLAN is used.

IPv4 address source

Here you select how the IPv4 address of the interface is to be obtained.

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

IPv6 address source

Here you select how the IPv6 address of the interface is to be obtained:

Router-Advertisement

The IPv6 address is derived from router advertisements that the device receives on the respective interface.

If the flag in the router advertisement is set to Other and/or Managed, additional configuration options are obtained via DHCPv6—even if the address source is set to **Router-Advertisement**.

DHCPv6

The IPv6 address is obtained via DHCPv6.

Static

The static IPv6 address configured for the interface is used.

Static IPv4 address

Here you configure the IP address to be used when the IPv4-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. “/24”) as a suffix.

Static IPv6 address

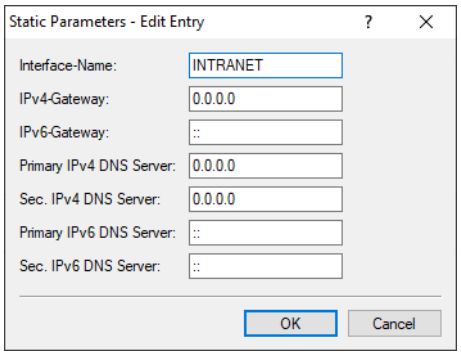
Here you configure the IP address to be used when the IPv6-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. “/64”) as a suffix.

Comment

Here you can enter a comment about the interface configuration.

4.4.2 Static parameters

Other settings related to the IP and network configuration that are required when using static IP addresses are located under **IP Configuration** > **Configuration** > **Static parameters**.



The settings made in this table only come into effect if the IPv4 or IPv6 address source for the corresponding LAN interface is set to **static**. Otherwise all of the necessary information is retrieved via DHCP, for example, in which case no configuration is required here.

Interface name

Enter the name of the interface, which the other settings made here refer to.

IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Primary IPv4 DNS server

Here you configure the primary IPv4 DNS gateway for the referenced interface.

Secondary IPv4 DNS server

Here you configure the secondary IPv4 DNS gateway for the referenced interface.

Primary IPv6 DNS server

Here you configure the primary IPv6 DNS gateway for the referenced interface.

Secondary IPv6 DNS server

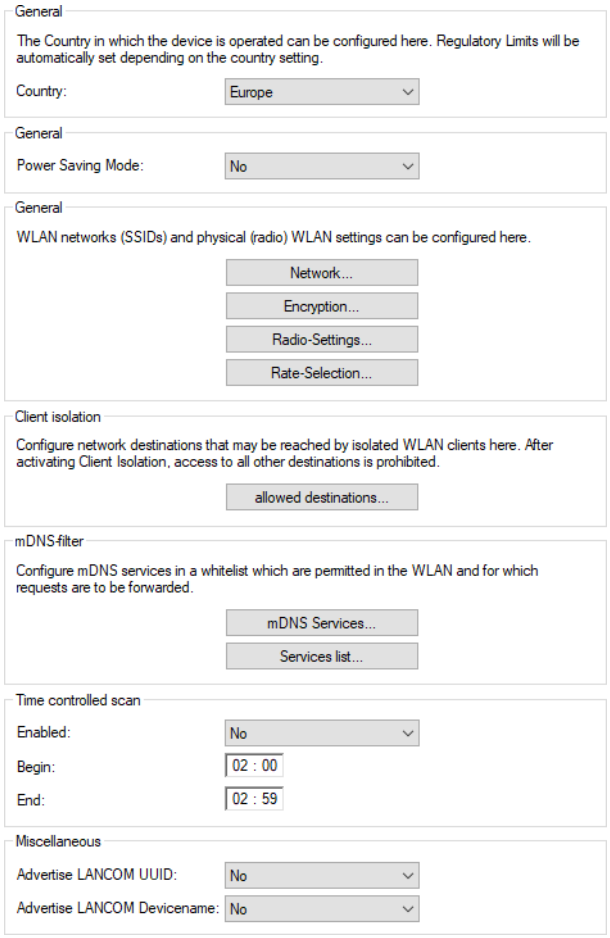
Here you configure the secondary IPv6 DNS gateway for the referenced interface.

4.5 Wireless LAN

In the section **Wireless LAN** you will find all the settings related to the broadcasting of WLAN networks.

4.5.1 WLAN networks

The wireless network settings for your device are located under **Wireless LAN** > **WLAN networks**.



General

Country

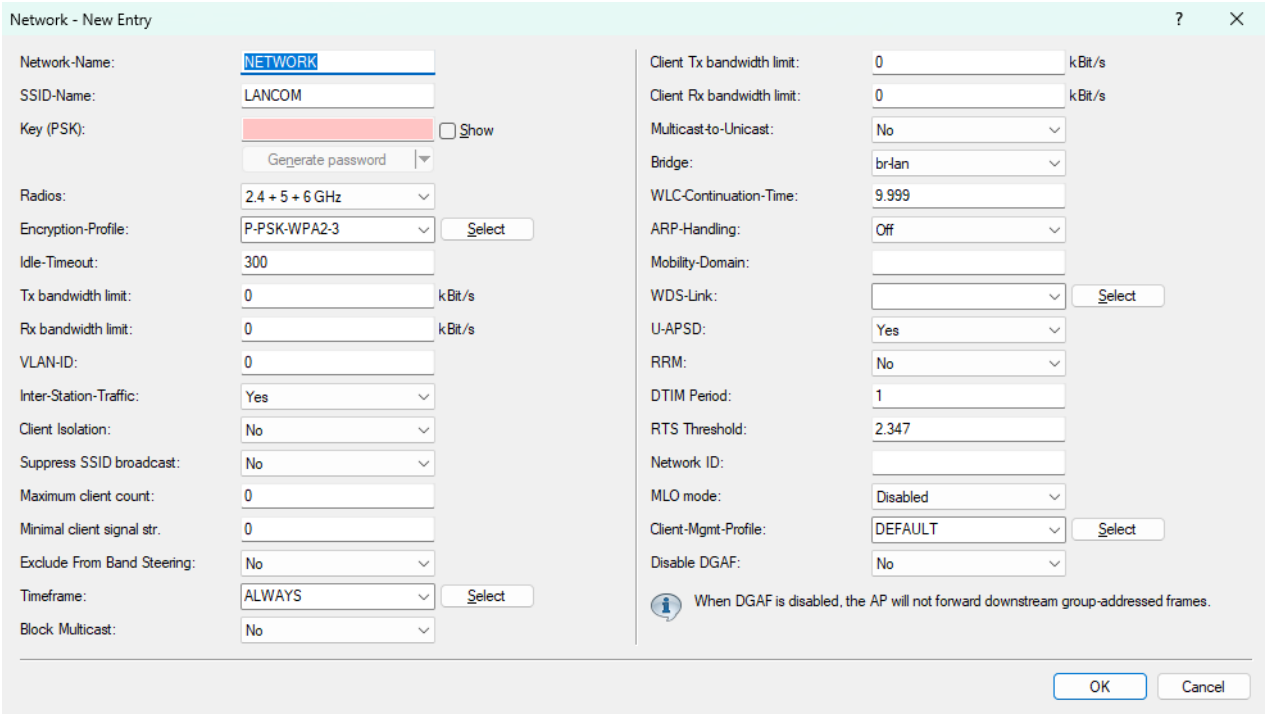
Here you configure the country where the device is operated. Depending on this, the appropriate regulatory limits are set automatically.

Power-saving mode

If the WLAN power saving mode is activated and no client is logged in, the access point reduces the number of active WLAN streams to 1 per radio. As soon as at least one client is connected to the radio, the number of active streams is increased again to the maximum possible for this radio.

4.5.1.1 Networks

General settings relating to the broadcast WLAN networks (SSIDs) are configured under **Wireless-LAN** > **WLAN-Networks** > **Network**. Add a line to the table for each WLAN network. By default, the table is empty.



Network-Name

Choose a meaningful name for the WLAN network here. This **internal** identifier is used to reference the interface configuration from other parts of the configuration.

This is **not** the name of the SSID and is not displayed by the clients. This is configured in the next step.

SSID-Name

Here you configure the name of the SSID to be broadcast. This name is displayed on the wireless clients when searching for WLAN networks.

Key (PSK)

Configure the pre-shared key (PSK) used for the WLAN network here. If you select **Show**, you can use **Generate password** to create a random password. Use the arrow next to it to set the strength, length and various other settings for the characters used for the generated pre-shared key.

This entry only applies if an encryption profile using WPA(2)-PSK or WEP is selected (please note, that WEP is insecure and is only supported to ensure downward compatibility. However, Rohde & Schwarz Networks and Cybersecurity GmbH explicitly recommends using WPA2 or WPA3). If 802.1X is used, the entry has no effect and the field can be left blank.

The following restrictions must be considered when using the encryption method WEP:

- WEP-40-Bits / WEP-40-Bits-802.1X – Any 5 characters from the allowed set of characters OR 10 HEX characters
- WEP-104-Bits / WEP-104-Bits-802.1X – Any 13 characters from the allowed set of characters OR 26 HEX characters
- WEP-128-Bits / WEP-128-Bits-802.1X – Any 16 characters from the allowed set of characters OR 32 HEX characters

Radios

Configure here the WLAN frequencies that the SSID is to be broadcast on.

2.4 GHz

The SSID is only broadcast on the 2.4 GHz frequency.

5 GHz

The SSID is only broadcast on the 5 GHz frequency.

6 GHz

The SSID is only broadcast on the 6 GHz frequency.

“Combinations”

The SSID is only broadcast on the specified frequency.

none

The SSID will not be broadcast. This can be used as a general on/off switch for the SSID.

Encryption-Profile

Here you select an encryption profile that defines the authentication and encryption method used for the SSID.

By default, the following encryption profiles are available for selection:

P-NONE

No encryption, the SSID is open.

P-PSK-WPA2

The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.

P-PSK-WiFi7

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled

› Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile “P-PSK-WiFi7” is included in the configuration as of LCOS LX 7.10 and can be used.

Idle-Timeout

This is the time in seconds during which the access point cannot receive any further packets after a client is disconnected. The timeout is reset by any data traffic from the client.

TX bandwidth limit

Here you set a WLAN bandwidth limit that applies to the entire WLAN network. All of the logged in clients can only receive data with the transmission rate configured here. The value “0” means that no limitation is active. The transmission direction is considered relative to the access point, so “Tx” means the transmission rate from the access point to the client. This setting affects the download rate at the client.

RX bandwidth limit

Here you set a WLAN bandwidth limit that applies to the entire WLAN network. All of the logged in clients can only send data with the transmission rate configured here. The value “0” means that no limitation is active. The transmission direction is considered relative to the access point, so “Rx” means the transmission rate from the client to the access point. This setting affects the upload rate at the client.

VLAN-ID

This VLAN ID is used to tag the data packets arriving from the WLAN and heading for the LAN. Similarly, packets with this VLAN ID arriving from the LAN are directed to the WLAN and are de-tagged.



This operating mode corresponds to what is normally known as the “Access” tagging mode, since it is assumed that wireless clients usually transmit data untagged. Tagging mode cannot be adjusted.

Inter-Station-Traffic

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. Here you configure whether communication between the WLAN clients on the WLAN network should be allowed.



Communication between WLAN clients can only be prevented within the SSID on one access point. If the communication should also be prevented across multiple access points, additionally the **Client Isolation** has to be configured.

Client Isolation

Client isolation can be switched on here for each SSID. See also *Client Isolation* on page 77.

Suppress SSID broadcast

Here you configure whether this SSID is displayed to clients searching for a network.

If the SSID broadcast is suppressed, the access point will not respond to probe requests with an empty SSID. In this case, establishing a connection requires the SSID to be explicitly entered into and configured on the client.

Maximum client count

This number determines the number of clients that can log on to the WLAN network simultaneously before further requesting clients are rejected.

The value “0” means that there is no limit, so unlimited number of clients can be logged in at the same time (up to a possible hardware-related limit).

Minimal client signal strength

Here you configure the minimum signal strength in percent that a client must “show” at the access point in order for it to be able to connect to the WLAN.

The value “0” means that there is no minimum signal strength requirement and clients are always allowed to connect.

Exclude From Client Management

This SSID may be exempted from the band steering.

Timeframe

Enter the name of a *Timeframe* here. This is used to schedule when this SSID is switched on or off.

Block-Multicast

This can be used to block multicasts sent or received by WLAN clients. A distinction can be made between IPv4 and IPv6.

ICMPv6 packets are not blocked in order for IPv6 address referencing to continue to work.

The LW-500 does not support this feature.

Client Tx bandwidth limit

Here you limit the bandwidth used by WLAN clients in the send direction.

Client Rx bandwidth limit

Here you limit the bandwidth used by WLAN clients in the receive direction.

Multicast-to-Unicast

For each WLAN network, you individually configure whether and how multicasts are converted into unicasts.

No

No conversion

Convert to unicast

Multicasts are converted to unicasts (layer-2 unicast on the WLAN layer with a unicast MAC address as destination). This corresponds to the behavior in the LCOS.

Encapsulate in Unicast Aggregate

Multicasts are encapsulated in unicast aggregates (A-MSDU with unicast MAC address as destination and containing a single layer-2 multicast). This variant should be used where target applications check the destination MAC address. However, note that aggregates are not supported by 802.11a/b/g clients.

In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine

which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

Bridge

Used internally in WLC mode or when operating *Layer-3 Ethernet tunnel with L2TPv3* on page 48, the L2TP interface must be entered here.

WLC-Continuation-Time

This value is written by a WLAN controller, if operating.

ARP-Handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If “ARP handling” is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point determines the assignment between IP address and MAC address from the DHCP messages that are either exchanged between WLAN client and DHCP server or ARP requests of the connected WLAN clients are evaluated or ARP requests from the connected WLAN clients, so-called gratuitous ARP requests or ARP replies are evaluated. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to “On”.

If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to “Strict”. This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

Off

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are forwarded to the WLAN.

Strict

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are not forwarded to the WLAN.

WDS-Link

Here you choose to broadcast specific SSIDs over WDS links. Also see *Links* on page 81.

If you wish to implement the repeater mode, this configuration must also be duplicated on the remote access point that is connected via WDS.

U-APSD

Automatic Power Save Delivery (APSD) is an extension of the IEEE 802.11e standard. APSD is offered in two variants:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

The two methods differ, among other things, in the use of the transmission channels. R&S®NC access points and wireless routers support U-APSD, on which the WMM Power Save (WMM-PS) method is also based. U-APSD enables significant power savings for WLAN devices. There is a particularly high demand for this function due to the increasing use of WLAN-enabled telephones (Voice over WLAN – VoWLAN).

By activating the U-APSD for a WLAN, the WLAN devices can switch to snooze mode during calls while they wait for the next data packet. VoIP data transmission takes place in a fixed time pattern—the WLAN devices synchronize their active phases with this cycle so that they are ready again in good time before the next packet is received. This significantly reduces power consumption and noticeably increases battery life.

RRM

The IEEE 802.11k standard describes a way to inform WLAN clients about potential roaming destinations, i.e., other access points of the same SSID within range (Radio Resource Measurement). This information to the client is provided by the “Neighbor Report” defined in the standard. Activate this option here.

DTIM Period

The DTIM period can be configured via SSID.

MLO mode

With Multi-Link Operation (MLO), Wi-Fi 7-capable WLAN clients can manage multiple associations with the same access point simultaneously. This increases throughput and reduces latency.

For WLAN clients with only one radio module, it is possible to switch quickly between the better-quality frequency bands. This significantly reduces disconnections in high-density wireless environments and provides more stable WLAN connectivity.

WLAN clients with multiple radios can use several frequency bands simultaneously to maximize data throughput.

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile “P-PSK-WiFi7” is included in the configuration as of LCOS LX 7.10 and can be used.

Since some of these settings may cause compatibility issues with existing (legacy) clients, we recommend configuring a separate SSID for Wi-Fi 7, MLO, and the above-mentioned encryption settings, and using it exclusively with Wi-Fi 7 clients.

Possible values:

Auto

MLO is enabled for all Wi-Fi 7 / IEEE 802.11be-capable radios where the SSID is broadcast.

Single-Link

Each Wi-Fi 7 / IEEE 802.11be-capable radio is treated as a standalone MLD (Multi-Link Device). In this case, the MLO “infrastructure” is used, but the radios remain separated. This mode may be useful in cases of compatibility issues.

Disabled

MLO is not used. The radios are not configured as MLDs.

Client Management Profile

Select one of the Client Management profiles under **Wireless LAN** > **Client Management** > **Profiles**.

4.5.1.2 Encryption

The settings for encryption and authentication on the WLAN networks are configured under **Wireless-LAN** > **WLAN-Networks** > **Encryption**. The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-NONE

No encryption, the SSID is open.

P-PSK-WPA2

The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

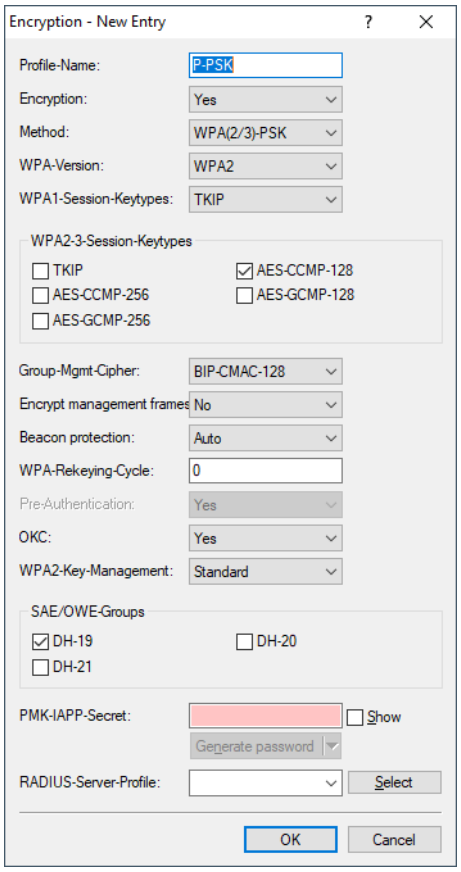
The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.

P-PSK-WiFi7

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile “P-PSK-WiFi7” is included in the configuration as of LCOS LX 7.10 and can be used.



Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

Encryption

Here you configure whether the WLAN network should be encrypted or if no encryption should be used (Open Network).

Method

Here you configure the encryption method. The following methods are available:

WPA

- WPA(2/3)-PSK: WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal.
- WPA(2/3)-802.1X: WPA2 and/or WPA3 with 802.1X, also known as WPA-Enterprise

Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP

The WEP process no longer provides adequate security and should only be used to integrate legacy clients that do not support a newer security method. If this is

the case, we recommend that you isolate the WEP clients in their own VLAN to keep them separate from the rest of the WLAN infrastructure.

- WEP-40-Bits: WEP with 40-bits key length
- WEP-104-Bits: WEP with 104-bits key length
- WEP-128-Bits: WEP with 128-bits key length
- WEP-40-Bits-802.1X: WEP with 40-bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

- WEP-104-Bits-802.1X: WEP with 104-bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

- WEP-128-Bits-802.1X: WEP with 128-bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

Enhanced-Open

Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. What also offers only limited security is the widespread practice of securing a hotspot with WPA2-PSK and publicly announcing the shared key, for example, on a poster. Since WPA2-PSK does not offer Perfect Forward Secrecy, an attacker who knows this key can use it to subsequently decrypt recordings of secure data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot. Just set the encryption method. That is all you need to do to encrypt communications for clients that support this method.

Clients, which don't support the encryption method **Enhanced-Open** cannot connect to the WiFi network.

WPA-Version

Wi-Fi Protected Access (WPA) is an encryption method. Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA3: WPA version 3 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.
- WPA2/3: Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

WPA2/3-Session-Keytypes

Configure here which session key type should be offered for WPA version 2 or 3. This also influences the encryption method used. The following types are available for selection:

TKIP

TKIP encryption is offered.

AES-CCMP-128

This procedure of the Advanced Encryption Standard (AES) is offered.

AES-CCMP-256

This procedure of the Advanced Encryption Standard (AES) is offered.

AES-GCMP-128

This procedure of the Advanced Encryption Standard (AES) is offered.

AES-GCMP-256

This procedure of the Advanced Encryption Standard (AES) is offered.

For maximum compatibility with legacy clients, the sole setting AES-CCMP-128 should be used. Please note that IEEE 802.11be standard-compliant operation requires the use of AES-GCMP-256. Based on experience, current Wi-Fi 7 clients also support other encryption methods, such as AES-CCMP-128, or combinations thereof. This is especially important when operating mixed SSIDs for Wi-Fi 7 and older clients, which generally only support AES-CCMP-128. If in doubt, use a separate SSID for Wi-Fi 7 with the appropriate encryption settings.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

Encrypt management frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don't have the corresponding key.

As of WPA3, management frames have to be encrypted, so this value is ignored there and is assumed to be set as "Mandatory". For WPA2, this is optional.

Beacon Protection

The IEEE 802.11be (Wi-Fi 7) standard stipulates the use of beacon protection. This can be configured here.

The preset "Auto" mode automatically switches Beacon Protection on for all radios that support IEEE 802.11be. To increase compatibility with legacy clients, it may be necessary to switch off Beacon Protection.

WPA-Rekeying-Cycle

A 48-bit long initialization vector (IV) impedes attackers in their attempts to calculate the WPA key. WPA also introduced the use of a new key for every data packet (per-packet key mixing and re-keying). The actual key, consisting of the IV and WPA key, is only repeated every 16 million packets. In high-traffic WLANs, the key is repeated only after several hours. To avoid repetition of the key, WPA automatically renegotiates the key at regular intervals. This avoids the repetition of the actual key.

Here you configure the time in seconds after which the access point performs rekeying when operating a version of WPA.

The standard value is "0" and the key is not negotiated in advance.

Pre-Authentication

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the access point previously. The WLAN client uses pre-authentication to reduce the time to logon to the access point at the first logon attempt.

Usually, a WLAN client carries out a background scan of the environment to find existing access points that it could connect to. Access points that support WPA2/802.1X can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1X authentication as follows:

- The WLAN client logs on to the new access point via the infrastructure network, which interconnects the access points. This can be an Ethernet connection or a WDS link (wireless distribution system), or a combination of both connection types.
- A pre-authentication is distinguished from a normal 802.1X authentication by the differing Ethernet protocol (EtherType). This allows the current access point and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new access point and the WLAN client.

  The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.
- When the client wants to connect to the new access point, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the PMK caching.

OKC (Opportunistic Key Caching)

This option enables or disables the opportunistic key caching (OKC).

The authentication of WLAN clients via EAP and 802.1X is now standard in company networks, and for public Internet access, too, it is part of the Hotspot 2.0 specification. The disadvantage of authentication via 802.1X is the noticeably longer time between authenticating and connecting due to the exchange of up to twelve data packets between the WLAN client and access point. This may not matter for most applications that only involve exchanging data. However, time-critical applications such as Voice-over-IP rely on fast authentication when moving between WLAN radio cells so as not to impair communications.

Various authentication strategies have been established to counteract this, including PMK caching and pre-authentication, although pre-authentication by no means solves all of the problems. For one thing, there is no guarantee that the WLAN client can detect whether the access point is capable of pre-authentication. Also, pre-authentication causes a considerable load on the RADIUS server, because it has to process the authentications of all clients and all access points on the WLAN network.

With opportunistic key caching, the management of WLAN client keys is moved to a WLAN controller (WLC) or central switch, which manages all of the access points in the network. When a client authenticates at an access point, the downstream WLC, which acts as the authenticator, performs the key management and returns the PMK to the access point for forwarding to the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID, and it sends this to the new access point in the expectation that OKC is enabled (i.e. “opportunistic”). If the access point is unable to handle the PMKID, it negotiates a regular 802.1X authentication with the client.

A R&S®NC access point is even able to perform OKC if the WLC is temporarily unavailable. In this case it stores the PMK and sends it to the WLC, once available again. The WLC then sends the PMK to all of the access points in the network so that the client can continue to use OKC when moving between cells.

In networks managed from the R&S®LANCOM Management Cloud (LMC) or networks from standalone access points, the PMKs are transmitted via the IAPP protocol. In LMC-managed networks, the IAPP is configured automatically. In networks made up with standalone access points, you have to ensure that the PMK-IAPP secret is configured and identical on every access point in the network.

WPA2-Key-Management

Here you specify which standard the WPA2 key management should follow. Possible values:

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard. See also *Fast roaming* on page 16.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Standard+Fast-Roaming

Combination of standard and fast roaming

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

SAE/OWE groups

Contains the selection of the available Diffie-Hellman groups used by the protocol partners to create a key for exchanging data. The available groups use elliptical curves.

The authentication method SAE (Simultaneous Authentication of Equals) used by WPA3 uses these methods together with AES to generate a cryptographically strong key.

DH-19

256-bit random ECP group

DH-20

384-bit random ECP group

DH-21

521-bit random ECP group

PMK-IAPP-Secret

This passphrase is used to implement encrypted opportunistic key caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

RADIUS-Server-Profile

Here you configure the RADIUS server profile used when operating 802.1X. No input is required when using PSK-based encryption methods. The profiles are created under *RADIUS* on page 86.

Note on WLAN encryption in the 6 GHz band

Since the 6 GHz band is a completely new frequency band, backwards compatibility with older clients is not necessary. Similarly, outdated security methods are not supported. Specifically, this means

- that network encryption is exclusively based on WPA3. Accordingly, no transition mode or mixed mode such as WPA2/3 is available.
- Using Enhanced Open for “open” networks (which thus offer encryption of the transmitted data). It is no longer possible to use open, unencrypted SSIDs.
- Protected Management Frames are mandatory

The conditions mentioned above can be set in the LCOS LX configuration. If an explicit configuration is not desired or possible (e.g. with mixed operation of the same SSID on several bands, which is a common application), the following adjustments are made dynamically by LCOS LX as soon as an SSID on the 6 GHz band is to be used:

- WPA versions <3 are automatically switched to WPA3
- Enhanced Open is enabled for open networks

› Protected Management Frames is activated

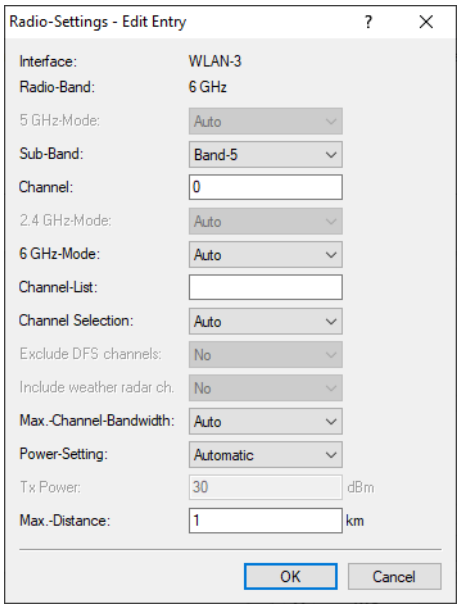
This makes it possible to continue using existing encryption profiles and to use a common configuration for an SSID that is also to be broadcast on 6 GHz. These settings are dynamically adjusted during operation, and there is no change to the configuration stored in the device.

4.5.1.3 Radio settings

Settings relating to the physical radio parameters are configured under **Wireless LAN** > **WLAN networks** > **Radio settings**. By default, there is an entry in the table for every physical WLAN radio for modification as required.

For compatible access points, this table contains an additional entry “WLAN-3” for configuring the 6-GHz WLAN radio.

As with the 2.4-GHz and 5-GHz radios, the frequency band cannot be changed. The radio WLAN-3 only supports the 6-GHz band.



Interface

The internal name of the WLAN radio. This cannot be changed.

Radio band

Shows whether this interface is operating in the 2.4-GHz, 5-GHz or 6-GHz frequency range.

5-GHz mode

Here you configure the mode used for 5-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Auto

All modes supported by the device are used.

11an-mixed

The modes 802.11a and 802.11n are used.

11anac-mixed

The modes 802.11a, 802.11n and 802.11ac are used.

11nac-mixed

The modes 802.11n and 802.11ac are used.

11ac-only

Only the 802.11ac mode is used.

11anacax-mixed

The modes 802.11a, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6) are used.

11anacaxbe-mixed

The modes 802.11a, 802.11n, 802.11ac, 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) are used.

Maximum compatibility and performance is available by setting the mode to **Auto**.

Sub-Band

Here you configure which sub-bands are used in the 5-GHz mode. The following sub-bands are available:

Band-1

Only sub-band 1 is used. This corresponds to the WLAN channels 36, 40, 44, 48, 52, 56, 60 and 64.

Band-2

Only sub-band 2 is used. This corresponds to the WLAN channels 100, 104, 108, 112, 116, 132, 136 and 140.

Band-1+2

Both sub-band 1 and sub-band 2 are used.

Band-5

The designation Band-5 is based on the FCC's U-NII nomenclature and corresponds to Band U-NII-5. In the EU, only the 5.925–6.425 MHz frequency range is approved for WLAN in the 6-GHz band (which corresponds to Band 5 or U-NII-5).

WLAN channels 120, 124 and 128 are not used because these channels are reserved for the primary user RADAR.

Channel

Here you configure the channel to be used for WLAN radio operations.

The value “0” allows the automatic selection of a suitable channel.

With automatic channel selection, the channel is not changed during operation. The channel is only selected when the WLAN module starts.

In 5-GHz mode, the channel set here represents a preferred channel. However, since the 5-GHz band requires the use of Dynamic Frequency Selection (DFS), there is no guarantee that the preferred channel will actually be used.

In the 6-GHz band, the following channels can be configured in LCOS LX:

1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93

These channels are 20 MHz wide. If a channel width greater than 20 MHz is selected (default setting for the 6-GHz band: 160 MHz), the channel set here becomes the primary channel for the wider channel. In this way, the primary channel can also be freely selected within a >20 MHz-wide channel; all you have to do is enter the desired 20 MHz channel.

2.4-GHz mode

Here you configure the mode used for 2.4-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Auto

All modes supported by the device are available, except for 802.11b.

11bg-mixed

The modes 802.11b and 802.11g are used.

11g-only

Only the 802.11g mode is used.

11bgn-mixed

The modes 802.11b, 802.11g and 802.11n are used.

11gn-mixed

The modes 802.11g and 802.11n are used.

11bgnax-mixed

The modes 802.11b, 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

11gnax-mixed

The modes 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

Maximum compatibility and performance is available by setting the mode to **Auto**.

6-GHz mode

Here you configure the mode used for 6-GHz radio operation. The following modes are available:

Auto

All modes supported by the device are used.

802.11ax

The mode used is 802.11ax (Wi-Fi 6E).

11axbe-mixed

The modes 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) are used.

Maximum compatibility and performance is available by setting the mode to **Auto**.

Channel list

Here you configure a comma-separated list of further WLAN channels. Automatic channel selection selects a channel from this list, rather than from the full range of supported WLAN channels.

Channel selection

Networks operating without manual WLAN channel planning or ARC 2.0 use automatic channel selection, which evaluates the WLAN channel based on quality criteria such as channel load, interference, and other SSIDs on that channel. If the access points in this type of network are all started at the same time, e.g. after a power failure, all of the access points will assess the channel quality and could well all come to the same result. In this case many access points will end up working on the same channel, which in some scenarios may be problematic. Random WLAN channel selection after restarting will ensure that the distribution is as even as possible in larger networks, with little multiple occupancy of any channels.

R&S®NC recommends the use of LMC-supported channel planning via ARC 2.0, or to conduct manual planning based on a site survey.

Exclude DFS channels

Here you configure whether to use channels in the 5-GHz band that require Dynamic Frequency Selection (DFS).

If these channels are excluded here, the channels still available in the 5-GHz band are 36, 40, 44 and 48. Since DFS is not required for these channels, they can be set with the option **Exclude DFS channels** in the radio channel and also in the **Channel list**.

Include weather radar channels

Automatic channel selection allows for the channels 120, 124 and 128 used by the weather radar in the frequency range 5.6 to 5.65 MHz. If one of the channels is used, the DFS scan time (CAC time) increases from 1 to 10 minutes. During the scan, the 5-GHz radio cannot be reached by WLAN clients.

Max. channel bandwidth

Here you configure the maximum allowed channel bandwidth. The following settings are available:

Auto

For a 2.4-GHz radio the channel bandwidth of 20 MHz is always used. For a 5-GHz radio the maximum possible channel bandwidth (up to 80 MHz) is used,. For a 6-GHz radio the maximum possible channel bandwidth (up to 320 MHz) is used. If desired, the channel bandwidth can be further restricted here by using one of the other values.

20 MHz

The channel bandwidth is always 20 MHz.

40 MHz

Depending on the environment, channel bandwidth is up to 40 MHz, but this can also fall back to 20 MHz.

80 MHz

Depending on the environment, channel bandwidth is up to 80 MHz, but this can also fall back to 40 MHz or 20 MHz.

160 MHz

Depending on the environment, channel bandwidth is up to 160 MHz, but this can also fall back to 80 MHz, 40 MHz or 20 MHz.

320 MHz

Depending on the environment, channel bandwidth is up to 320 MHz, but this can also fall back to 160 MHz, 80 MHz, 40 MHz or 20 MHz.

Antenna gain

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly. Here you enter the gain of the antenna minus the actual cable loss. For an AirLancer Extender O-18a antenna with a gain of 18 dBi and a 4 m cable with a loss of 1 dB/m, the 'Antenna gain' would be entered as 18 - 4 = 14. This value for true antenna gain is dynamically used to calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.

Available for devices with external antennas only.

Antenna mask

The antenna mask settings are only available for devices with external or removable antennas.

This setting helps when using WLAN antennas with a different number of streams than the access point (e.g., a two-stream antenna connected to a four-stream access point). This allows you to disable ports on the access point that are not connected to an antenna.

Power setting

This setting regulates whether to use the maximum permitted transmission power that the access-point hardware can achieve (“Automatic”) or to specify the desired target transmission power in manual mode (“Manual”). This is done in dBm in the field **Tx power**.

Tx power

Depending on the setting in the field **Power setting**, you set the transmission power in dBm here.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically.

Under no circumstances will the access point exceed the regulatory limits for transmission power. These are always respected automatically, regardless of the settings made here.

Max. distance

Enter the distance to the furthest WLAN station (e.g. to a WDS partner).

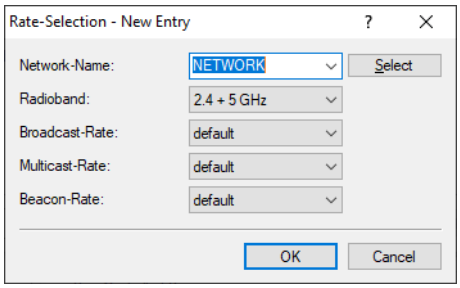
This setting increases the internal timeout for WLAN ACK packets so that packets from a distant station can be processed. Default is 1 kilometer.

4.5.1.4 Rate selection

Increasing the broadcast and multicast data rates can help to reduce the load on the medium. Broadcasts and multicasts are usually sent at the lowest possible rate in order to reach distant

clients; however, this means that they occupy a large slice of medium time. Adjusting this setting can be particularly useful in large networks with a high density of access points.

Configure the broadcast and multicast data rates under **Wireless-LAN** > **WLAN-Networks** > **Rate-Selection**.



Network-Name

The network or SSID to which the rates configured here should apply. The name must match with a name of a network set up in *Networks* on page 59.

Radioband

The band that the rates configured here apply to. This can be further limited to a specific band.

Broadcast-Rate

The rate to use for sending broadcasts.

If the broadcast rate is set to 6 Mbps, 12 Mbps, or 24 Mbps, this rate is also used for transmitting beacons.

Rates other than this only influence the broadcast packets but not the beacon rate.

Multicast-Rate

The rate to use for sending multicasts.

Beacon-Rate

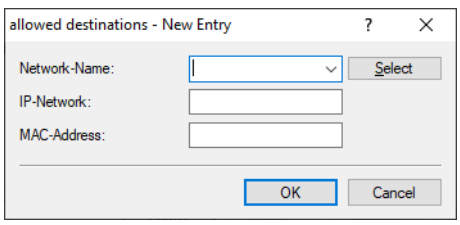
The data rate at which WLAN beacons are broadcast. In high-density scenarios, we recommend a higher data rate to save airtime.

4.5.1.5 Client Isolation

Client isolation prevents WLAN clients from communicating with one another or with unauthorized destinations on the network.

Data traffic from WLAN clients to destinations that are not explicitly whitelisted is prohibited.

Client isolation can be switched on per SSID. Configure this under **Wireless-LAN** > **WLAN-Networks** > **Network** > **Client Isolation**.Then configure the allowed destinations under **Wireless-LAN** > **WLAN-Networks** > **allowed destinations**.



Network name

Select the network / SSID that the entry should apply for. Then enter either a destination IP address or destination MAC address.

In hotspot scenarios, the MAC address of the gateway should be entered here to ensure Internet access. It is not sufficient to specify its IP address because in this scenario the destination IP address is that of a destination on the Internet.

The feature automatically determines the appropriate gateway address from a DHCP negotiation between a WLAN client and a DHCP server. However, in roaming scenarios there is usually no renewed DHCP negotiation during roaming, so in this case the gateway must be explicitly whitelisted.

IP network

Allowed destination IP address for this network.

MAC address

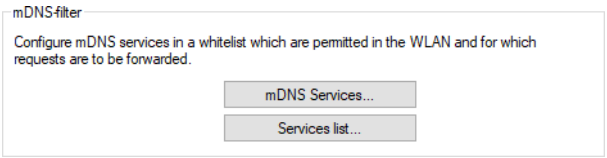
Allowed destination MAC address for this network.

4.5.1.6 mDNS filter

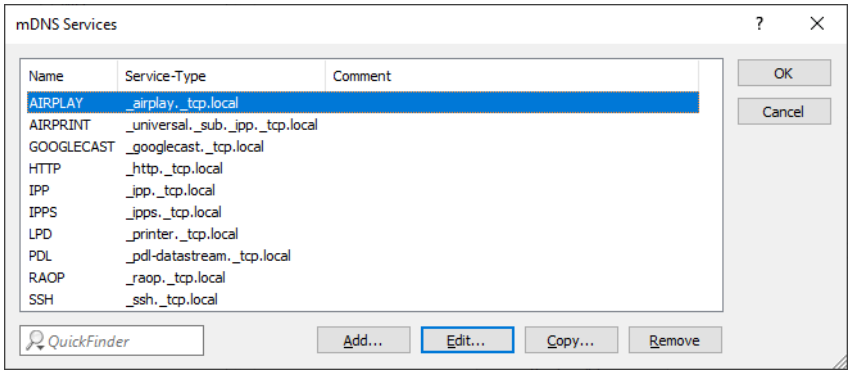
mDNS (Multicast DNS) is used for simple service discovery in the (W)LAN. Prominent applications based on this are Bonjour / AirPlay and Google Cast.

Since mDNS requests are sent as multicast, transmission at the WLAN level must use the lowest permitted data rate, which can consume significant airtime depending on the volume of mDNS requests. With the mDNS filter, requests to definable mDNS services can be selectively allowed for forwarding over the WLAN.

Configure the mDNS filter under **Wireless LAN** > **WLAN Networks** > **mDNS filter**.



mDNS Services contains the most common mDNS-based services by default, but it can also be manually extended.



Name

The name of a service.

Service-Type

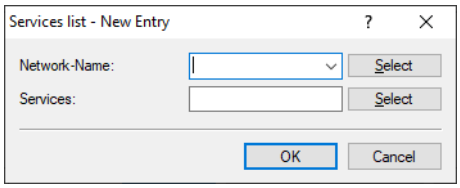
The type of this service.

Comment

Comment for this entry.

In the **Services list**, configure filters based on the services from the **mDNS Services** table.

The Services list works as a whitelist: If the list is not populated, all mDNS services are allowed. If the list contains entries, only the permitted services are allowed. All other services are filtered.



Network-Name

Here you can configure the WLAN network name for which the filter should apply.

Services

Here you can add one or more of the mDNS-based services defined in the Services table for which requests should be forwarded.

4.5.1.7 Miscellaneous

Advertise LANCOM UUID

All current R&S®NC access points are multi-SSID-capable. This means that they can offer different “virtual” access points to several WLAN clients at the same time.

In addition, for devices with two or more radio modules (dual radio), the BSSIDs of the logical networks refer to the corresponding radio module, but the MAC addresses of the two radio modules are completely independent of each other. This means that logical networks with different BSSIDs cannot be uniquely assigned to a device.

For network monitoring and planning, however, it is useful to be able to assign the logical networks to the corresponding devices (or radio modules) using tools such as Ekahau Site Survey.

R&S®NC access points have a UUID (Universally Unique Identifier), which is calculated from the device type and serial number and can uniquely identify the device in the network. However, encryption during UUID generation means that it is not possible to identify the device or serial number.

This option determines whether an access point transmits its UUID.

Advertise LANCOM device name

Configures whether an access point transmits its device name. To support WLAN site survey tools, the device name of the access point can be inserted into beacons. The name is identical for all radios of a multi-radio access point, so that the individual radios can be assigned to an access point by name.

The device name is coded as a vendor-specific info element as follows:

```
Tag: Vendor Specific: LANCOM Systems GmbH
  Tag Number: Vendor Specific (221)
    # 1 Byte (static value)
  Tag length: 13
    # 1 Byte (static length)
      # In this case: 3 Bytes OUI + 1 Byte LCS Subtype + 2 Bytes LCS Version + 7 Bytes LCS Devicename

  OUI: 00:a0:57 (LANCOM Systems GmbH)
    # 3 Bytes (static value)
  Vendor Specific OUI Type: 8
    # 1 Byte (static length)
      # LCS Subtype: 8 == Devicename
  Vendor Specific Data: 080100544553542d4150
    # Wireshark output comprising 1 Byte "Vendor Specific OUI Type" (0x08)
    # In this case: 9 Bytes
      # 2 Bytes (static value)
        # LCS Version: 1 (little-endian)
      # In this case: 7 Bytes
        # ASCII encoded String
          # In this case: 0x544553542d4150 == TEST-AP
```

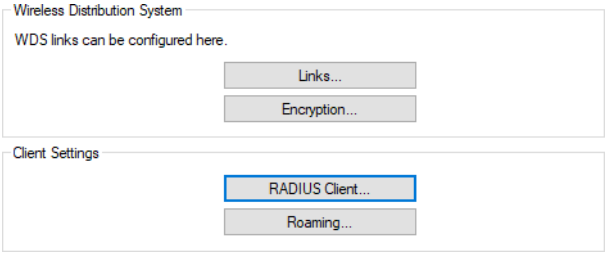
4.5.2 Wireless Distribution System (WDS) / point-to-point links

WDS can be used to set up point-to-point WLAN links between access points. These connections serve as a wireless backhaul, allowing remote access points to be connected to the rest of the network. This allows WLAN coverage to be provided even in areas where access points cannot be connected via Ethernet, for example.

These access points optionally offer SSIDs for connecting WLAN clients (“repeater” mode) or for connecting the wireless backhaul to its Ethernet port (wireless bridge).

With LCOS LX 6.10, WDS operation is validated over a maximum distance of 300 meters.

The WDS settings for your device are located under **Wireless-LAN** > **WDS**.



Transmitting WLAN networks

One option of the WLAN configuration is to broadcast specific SSIDs over WDS links. You do this under **Wireless-LAN** > **WLAN-Networks** > **Network** in the selection field **WDS-Link**.

If you wish to implement the repeater mode, this configuration must also be duplicated on the remote access point that is connected via WDS.

Radio settings

The general radio settings made for the access point also apply to WDS links (in particular the setting of the WLAN channel). Configure this in the usual way under **Wireless-LAN** > **WLAN-Networks** > **Radio-Settings**.

In particular, make sure that any specified channels or limitations to certain sub-bands match at both ends of the WDS link, otherwise the connection will not be established. Alternatively, automatic

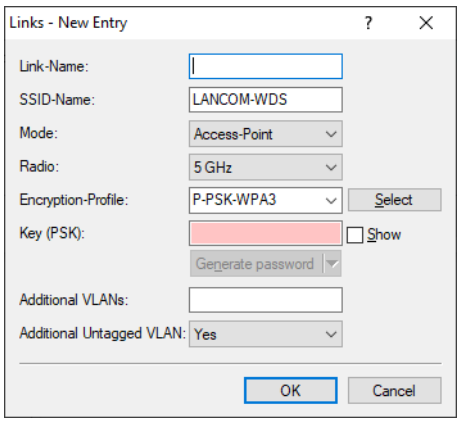
channel selection can be operated at both ends. In this case, the device searches through all permitted channels until the WDS partner is found.

Client mode for flexible integration of Ethernet-capable devices in wireless networks

The client mode allows access points to be used flexibly for integrating a wide range of Ethernet-capable devices into existing WLAN networks—independent of the operating system and thus regardless of the manufacturer. For customized security, you can choose between certificate-based encrypted communication via IEEE 802.1X or via WPA2/3-PSK. Setup is conveniently carried out via the modern WEBconfig user interface.

4.5.2.1 Links

General settings relating to the WDS connection are configured under **Wireless-LAN** > **WDS** > **Links**. Add a line to the table for each WDS connection. By default, the table is empty.



Link-Name

The name of the link. Used for further referencing in the device configuration.

SSID-Name

The name of the special SSID used for the WDS link. This name must match at both ends of the connection.

Mode

In the context of a WDS connection, there are three roles: Access Point, Client, Legacy Client. The partner configured as a client searches for a partner configured as an access point using the SSID configured above and initiates the connection. The access point configured as a legacy client can log into the SSID of any access point

In a point-to-multipoint scenario, multiple clients can connect to an access point.

The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above. In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

Encryption-Profile

The encryption profile to be used for the WDS link.

Key (PSK)

The WPA-PSK used for the WDS link. When using an encryption profile with 802.1X, this field can be left empty.

Additional VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

Additional Untagged VLAN

Untagged packets are to be transmitted.

LCOS Client Bridge Support

If the LCOS LX access point in client mode is connected to an LCOS access point in base station mode, 4-address frames can still be used for this, which enables the transmission of VLANs or MAC addresses. This mode cannot be used if the LCOS LX access point is operated in base station mode and an LCOS access point is logged in to it in client mode.

Roaming profile

Here you can enter a roaming profile if the access point is in client or legacy client mode.

Optionally configure an encryption profile under *Encryption* on page 82.

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first. See *RADIUS Client* on page 84

Create a roaming profile if required. See *Roaming* on page 85

4.5.2.2 Encryption

The settings for encryption and authentication of the Wireless Distribution System are configured under **Wireless-LAN** > **WDS** > **Encryption**.



For WDS connections, we recommend using WPA3 to guarantee maximum security.

The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-PSK-WPA2

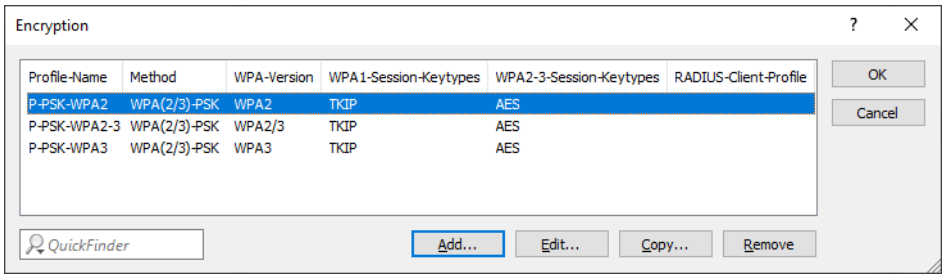
The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.



Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

Method

Here you configure the encryption method. The following methods are available:

WPA

WPA(2/3)-PSK: WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal.

RADIUS

WPA(2/3)-802.1X: WPA2 and/or WPA3 with RADIUS.

WPA-Version

Wi-Fi Protected Access (WPA) is an encryption method. Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA3: WPA version 3 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.
- WPA2/3: Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

WPA2/3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2 and 3. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

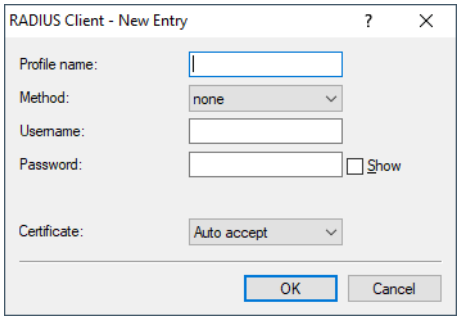
If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

RADIUS-Client-Profile

Specify a RADIUS client profile here if necessary.

4.5.2.3 RADIUS Client

The settings for logging in using 802.1X are configured under **Wireless-LAN** > **WDS** > **Client Settings** > **RADIUS Client**.



Profile name

Use a unique profile name, which you specify later in the encryption profile.

Method

Select a method that suits your requirement. When using “TLS”, uploading a certificate is necessary.

Username

Enter the RADIUS user name here. When using the “TLS” method, no entry is necessary here.

Password

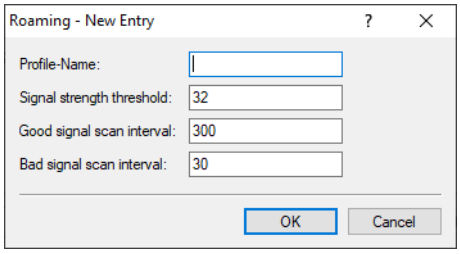
Enter the RADIUS password here. When using the “TLS” method, no entry is necessary here.

Certificate

You can accept the RADIUS server's certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server. The certificate upload is only possible in WEBconfig. See *Client certificate* on page 145.

4.5.2.4 Roaming

Settings relating to the roaming profile are configured under **Wireless-LAN** > **WDS** > **Client Settings** > **Roaming**.



Profile name

Use a unique profile name, which you specify later in the WDS connection.

Signal strength threshold

Enter the threshold value from which the scan interval of the access point should change. Values from 0 to 100 specify a percentage value. Values from -100 to 0 are in dbm.

Good signal scan interval

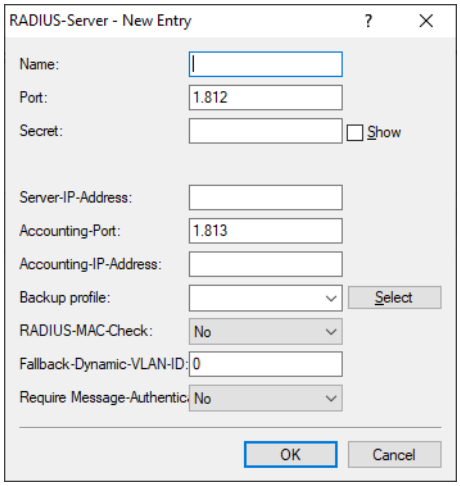
If the signal strength is above the limit, a scan is performed in seconds during this time to check if a better access point becomes available to connect.

Bad signal scan interval

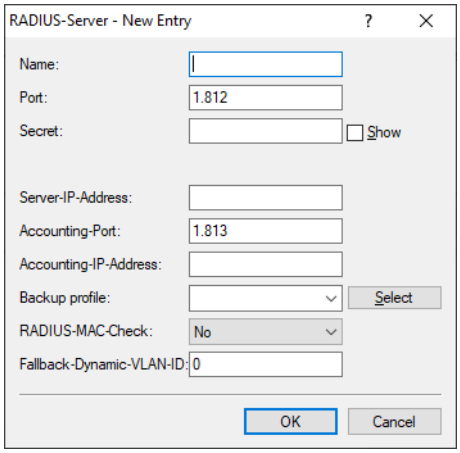
If the signal strength falls to the specified limit, a scan is triggered directly to search for a better access point. If no better access point is available, the search continues in the specified time in seconds until a connection to an access point with a better signal strength could be connected or the signal with the connected access point has improved again.

4.5.3 RADIUS

The settings for RADIUS server profiles when operating WLAN networks that use 802.1X as the authentication method can be found under **Wireless-LAN** > **RADIUS**.



Configure the RADIUS server profiles in the **RADIUS server** table.



Name

Choose a meaningful name for the RADIUS server profile here. This internal identifier is used to reference the RADIUS server profile from other parts of the configuration.

Port

Select the port (UDP) used to contact the RADIUS server.

This is usually the port 1812 (RADIUS authentication).

Secret

Here you configure the secret used to encrypt the traffic between the device and the RADIUS server. This secret must also be stored on the RADIUS server.

Server IP address

Here you configure the host name or IP address where the RADIUS server is to be reached.

Accounting port

Select the port (UDP) used to contact the RADIUS accounting server.

This is usually the port 1813 (RADIUS accounting).

Accounting IP address

Here you configure the host name or IP address where the RADIUS accounting server is to be reached.

Backup profile

Here you configure a backup profile, which will be used if the RADIUS server in the profile configured here cannot be reached.

RADIUS-MAC-Check

A user name can be authenticated with a MAC address instead of using the RADIUS server.

Require Message Authenticator

This option is used to specify whether a message authenticator is mandatory in RADIUS messages. If this is the case, messages without a message authenticator will not be processed and will be discarded.

4.5.3.1 Dynamic VLAN for 802.1X

The RADIUS server uses dynamic VLAN to assign a VLAN ID to the WLAN client for 802.1X authentication. This assigns clients to the required VLAN without the need to operate a separate SSID for each VLAN.

The RADIUS server must send the following attributes in the accept message:

ID	Name	Meaning	Possible values in LCOS LX
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	13 (VLAN)
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	6 (IEEE 802)
81	Tunnel-Private-Group-ID	Specifies a required VLAN ID.	1 – 4096

Specific issues when using RADIUS authentication with dynamic VLAN assignment on LCOS LX access points (802.1X):

If RADIUS authentication with dynamic VLAN assignment is to be configured, there are some special features to be considered for LCOS LX devices, which are *summarised in this Knowledge Base article*.

4.5.4 Client Management

Client management is used to distribute WLAN clients within a network across the available access points based on load. In high-density scenarios, this can result in a more even utilization of WLAN resources, including AP capacity and channel capacity.

Client management is based on two core technologies: RRM (Radio Resource Management / IEEE 802.11k) and WNM (Wireless Network Management (IEEE 802.11v).

RRM

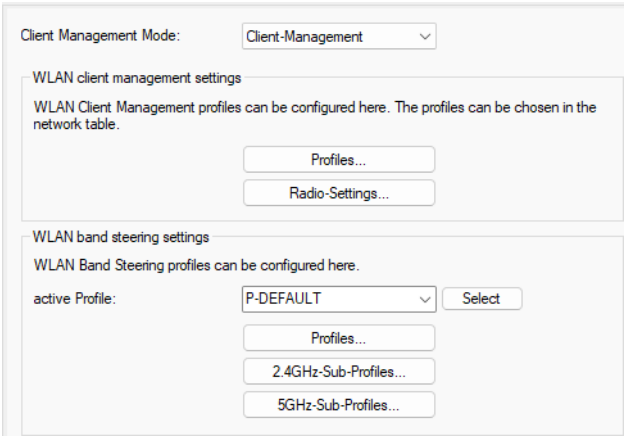
Client management supports RRM Neighbor Reports. Clients can send a Neighbor Report Request to the AP; the AP responds with a Neighbor Report containing a list of potential roaming candidates. The AP determines these roaming candidates by means of an automated environmental scan that is performed once a day, scans the radio environment for candidates, and uses IAPP to verify that the identified APs are in fact LCOS LX APs belonging to the same network. In addition to the list of candidates, a priority for each candidate is transmitted (BSS Transition Candidate Preference). This priority is based on the current number of clients associated with the candidate AP (fewer clients = higher priority).

WNM

Client management supports WNM BSS Transition Management (BTM). Clients can send BTM Queries to the AP, which in turn sends a BTM Request with one or more suitable roaming candidates. In principle, this is similar to the process described above for RRM; only a different protocol is used.

To instruct a client to switch to another AP, the AP can also send unsolicited BTM Requests to the client. This occurs as soon as the thresholds described below are reached. These thresholds are checked each time a new client associates. When a threshold is reached, Client Management randomly selects an associated client that has been associated for more than 5 minutes and sends it a BTM Request to encourage it to switch to a non-overloaded AP. Clients that have been associated for less than 5 minutes or that have already received a BTM Request from this AP within the last 5 minutes are not contacted in order to prevent multiple roaming processes within a short period of time.

You can find the Client Management settings for WLAN networks under **Wireless LAN** > **Client Management**.



Client Management Mode

Specify whether to use Client Management, band steering only, or neither feature.

4.5.4.1 Profiles

Under **Wireless LAN** > **Client management** > **Profiles**, define configuration profiles for client management or use one of the predefined profiles:

Existing Profiles

DEFAULT

Enables RRM, but not WNM/BSS Transition Management.

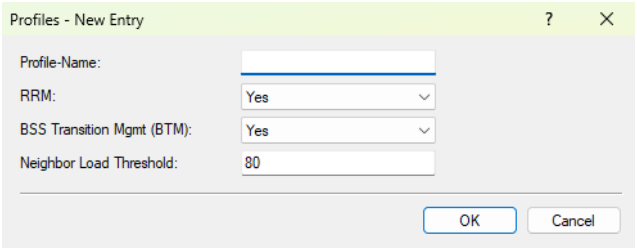
DISABLED

Disables both RRM and WNM/BTM.

RRM+BTM

Enables RRM and WNM/BTM.

Assign the desired profile under **Wireless-LAN** > **WLAN-Networks** > **Networks** > **Client-Mgmt-Profile**.



Profile-Name

Name of this profile.

RRM

Enable the use of RRM here.

BSS Transition Mgmt (BTM)

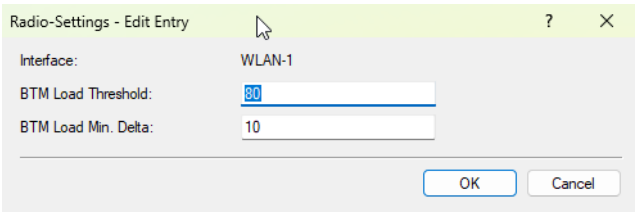
Enable the use of WNM/BTM here.

Neighbor Load Threshold

The percentage up to which APs may be loaded and still be considered as roaming targets. Currently, 100% corresponds to 80 associated clients; different AP models are not distinguished. The value is used for RRM and WNM/BTM.

4.5.4.2 Radio Settings

Under **Wireless-LAN** > **Client management** > **Radio-Settings**, define the radio settings for client management.



Interface

The WLAN interface to which the following settings apply.

BTM Load Threshold

When the load on this WLAN interface of the AP exceeds the threshold, the AP sends BTM requests to associated clients to steer them to other APs.

BTM Load Min. Delta

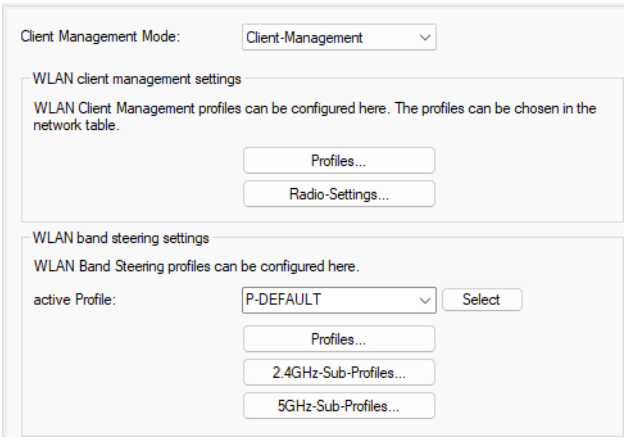
This is a dynamic threshold: it is relative to the load of the AP itself. The value configured here specifies the minimum load difference compared to our own load: only neighboring APs whose load is at least BTM Load Min. Delta lower than our own load are recommended to clients. All others are marked as “do not use”. Example: BTM Load

Threshold is 80, and BTM Load Min. Delta is 10. Assume that our own load is 85—we have exceeded the threshold and attempt to move clients to neighboring APs using BTM requests. However, with a minimum delta of 10, only APs whose load is at least 10 points lower than our own are recommended to clients. In this example, all neighboring APs with a load of 75 or higher are therefore marked as “do not use”. (Note: The static threshold from the profile table continues to apply independently.)

This “minimum delta” is used to create hysteresis and prevent two neighboring APs with a high load—each close to its own threshold—from continuously moving clients back and forth between them.

4.5.4.3 Band steering

The band steering settings for Wi-Fi networks can be found under **Wireless LAN** > **Client Management** > **WLAN band steering settings**.



Active profile

Here you select the profile with the settings for the band-steering module.

P-DEFAULT

Steering is based on the load on the medium and the interference detected on the current channel and is preferably performed with 802.11v. If the client does not support 802.11v, steering is induced by deliberately disassociating the client. Steering can be performed before association and, if necessary, once the client is already associated. This is the recommended profile.

P-DISABLED

No steering is performed. The client decides independently which frequency band to use.

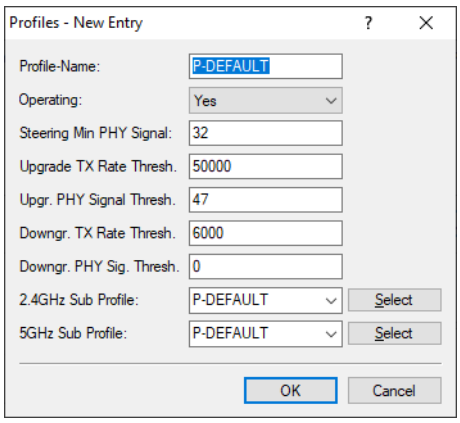
P-LEGACY

Steering is performed before the client associates by deliberately withholding probe responses. Regardless of the load, the 5 GHz band is always preferred.

4.5.4.3.1 Profiles

Adjust the detailed settings of the steering profiles or create a new profile under **Wireless LAN** > **Client Management** > **WLAN band steering settings** > **Profiles**.

R&S®NC recommends using the preset profiles.



Profile name

Give this profile a name.

Operation

Controls whether band steering is active for this profile.

Steering min. PHY signal

Specifies the client signal strength (in dB) below which client steering is initiated.

Upgrade TX rate threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 5 GHz band.

Upgrade PHY signal threshold

Specifies the client signal strength (in dB) required as a minimum before the client is considered for steering to the 5 GHz band.

Downgrade TX rate threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 2.4 GHz band.

Downgrade PHY signal threshold

Specifies the client signal strength (in dB) that must be exceeded before the client is considered for steering to the 2.4 GHz band.

For steering to 2.4 GHz (downgrade), the signal strength has to fall below the value configured here and also below the **Downgrade TX rate threshold** value.

2.4 GHz sub-profile

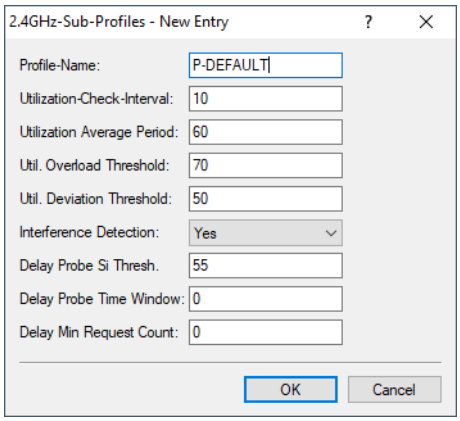
Here you configure which 2.4 GHz sub-profile is used.

5 GHz sub-profile

Here you configure which 5 GHz sub-profile is used.

4.5.4.3.2 2.4 GHz sub-profiles

The settings for the 2.4 GHz sub-profiles are located under **Wireless LAN** > **Client Management** > **WLAN band steering settings** > **2.4GHz sub-profiles**.



Profile name

Give this 2.4-GHz sub-profile a descriptive name.

Utilization check interval

Configures the interval (in seconds) for checking media utilization.

Utilization average period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the **Utilization check interval**.

Utilization overload threshold

Configures the media utilization (in percent) above which the current 2.4 GHz channel is assumed to be overloaded.

Utilization deviation threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

Interference detection

Configures whether interference on the configured 2.4 GHz channel is considered for steering decisions.

Delay probe signal threshold

Specifies the client signal strength (in dB) that must be reached before steering-related probe responses are delayed.

Delay probe time window

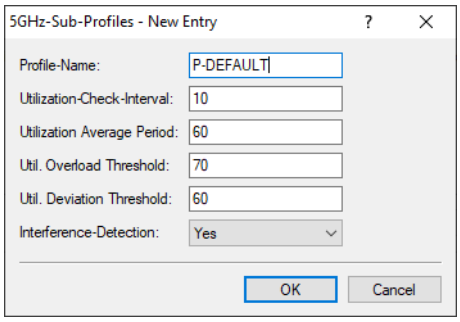
Configures the time window (in seconds) in which a client must receive at least the number of probe requests configured under **Delay min. request count** before it responds to them.

Delay min. request count

Configures the number of probe requests that a client must receive within the period configured under **Delay probe time window** before it responds to them.

4.5.4.3.3 5 GHz sub-profiles

The settings for the 5 GHz sub-profiles are located under **Wireless LAN** > **Client Management** > **WLAN band steering settings** > **5 GHz sub-profiles**.



Profile name

Give this 5-GHz sub-profile a descriptive name.

Utilization check interval

Configures the interval (in seconds) for checking media utilization.

Utilization average period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the **Utilization check interval**.

Utilization overload threshold

Configures the media utilization (in percent) above which the current 5 GHz channel is assumed to be overloaded.

Utilization deviation threshold

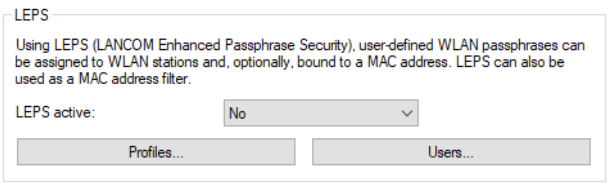
Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

Interference detection

Configures whether interference on the configured 5 GHz channel is considered for steering decisions.

4.5.5 Stations/LEPS

The configuration of the **Profiles** and **Users** for R&S®NC Enhanced Passphrase Security (LEPS) are located in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS**. The switch **LEPS active** enables the LEPS feature.



When configured in LEPS, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. LEPS profiles are used to avoid having to repeat all of the settings for every new user. You then create the LEPS users with their individual passphrases and link them to one of the LEPS profiles created previously.

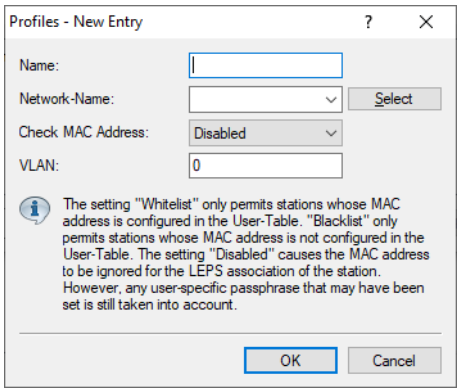
Alternatively, you can link the passphrase to a MAC address to set up a MAC address filter.

For technical reasons, LEPS is only compatible with WPA version WPA2.

Note that with WPA2/3 encryption mode, the client can use both WPA versions, which can lead to unexpected behavior when used with LEPS.

4.5.5.1 Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users.



Name

Enter a unique name for the LEPS profile here.

Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

Check MAC address

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

Only clients whose MAC address is not known are admitted.

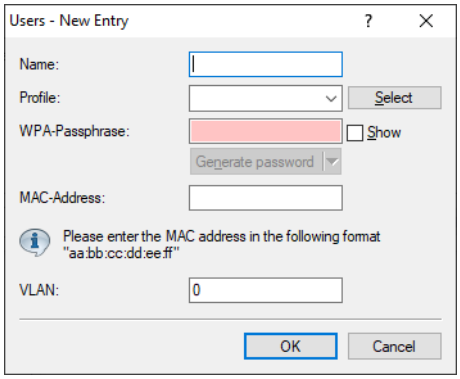
VLAN

Here you specify which VLAN is assigned to a LEPS user or client who is connected to this profile.

4.5.5.2 Users

Create individual LEPS users here. Each LEPS user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to

authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.



Name

Enter a unique name for the LEPS user here.

Profile

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

Compared to simply assigning a passphrase to a user, managing a passphrase for each MAC address requires a bit more work, but you have greater control over the devices in the network.

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN configured here takes priority.

4.5.6 WLC

LCOS LX-based access points can be managed by a R&S®NC WLAN controller (WLC). Like LCOS-based access points, they use the CAPWAP protocol.

The prerequisite for this is a R&S®NC WLAN controller with LCOS version 10.40 or higher.

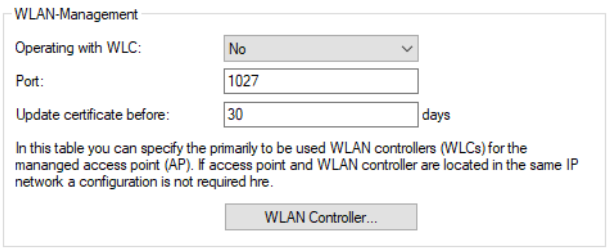
For background information on WLAN management with R&S®NC WLAN controllers, see the section “WLAN management” in the LCOS reference manual.

In their factory default settings, LCOS LX-based access points search the local network for a WLAN controller. They also query the DNS name “WLC-Address” to try to reach a WLAN controller.

An access point will not try to contact the R&S®LANCOM Management Cloud if it is already being managed by a WLC.

If the access point is managed by the R&S®LANCOM Management Cloud and a WLAN configuration is rolled out to the access point by the LMC in this context, the access point will no longer attempt to contact a WLC.

This make it possible to use zero-touch commissioning, which means that no further configuration of the access point is necessary. A manual configuration may still be necessary in certain circumstances. This can be done using LANconfig in the device configuration under **Wireless LAN** > **WLC**.



Operating with WLC

This configures whether an access point actively searches for a WLC and can be managed by one.

This option should be deactivated for operation in stand-alone mode.

Port

Configures the port used to attempt to reach a WLC. The default value of 1027 is the default port used by the CAPWAP protocol. By default, R&S®NC WLCs also use this port.

Update certificate before

Configures how many days before its expiry that the device certificate used by the access point to authenticate at the WLC is renewed.

WLAN Controller

Configures user-specified WLAN controllers. This may be necessary if a WLC cannot be found via the local network (e.g. with routed connections) and also the DNS name “WLC-Address” cannot be used to inform the access point about the address of the WLC.

4.5.6.1 Supported features

LCOS LX supports the following features for WLC operations (from the perspective of the WLAN controller):

Area	Feature	Supported?	Remarks
WLAN Controller > **General**	Password synchronization	Yes	
	WLAN scheduling	Yes	
	Specify alternative WLAN controller	No	

Area	Feature	Supported?	Remarks
WLAN Controller > **Profiles** > **Logical WLAN networks (SSIDs)**	LAN on the AP with VLAN tagging	Yes	
	WLC tunnel	Yes	From LCOS LX 5.32 Rel in conjunction with LCOS from 10.42 RU3 on the WLAN controller
	Encryption – WPA2	Yes	
	Encryption – WPA3	Yes	
	Encryption – Enhanced Open	Yes	
	Encryption – Enhanced Open Transitional	No	
	802.1X	Yes	
	RADIUS profile	Yes	
	2.4- / 5 GHz mode	Yes	
	Standalone mode	Yes	
	802.11u / Hotspot 2.0	No	
	OKC	Yes	
	MAC check	Yes	
	RADIUS accounting	Yes	
	Inter-station traffic	Yes	
	Fast roaming	Yes	
	Base rate adjustable	No	
	Client bridge support	No	
	Bandwidth limitation per SSID	Yes	
	Bandwidth limitation per client	Yes	The **Client TX bandwidth limit** does not work when using a WLC tunnel.
	Maximum count of clients	Yes	
	Min. client signal strength	Yes	
	Client disassociation signal strength	No	
	Location-based services (LBS)	No	
	Convert to unicast	Yes	LCOS LX cannot convert DHCP. So with the setting **DHCP** the unicast conversion in LCOS LX stays disabled and with **DHCP and multicast**, only multicast packets are converted to unicast.
	Transmit only unicasts	No	Broadcast packets cannot be discarded with LCOS LX.
	U-APSD	Activated permanently	

Area	Feature	Supported?	Remarks
	Encrypt mgmt frames	Yes	
WLAN-Controller > **Profiles** > **Physical WLAN parameters**	Country setting	Yes	
	Configure 2.4 GHz mode	Yes	If a setting for the 2.4 GHz band is selected but is not supported by the access point (e.g. 802.11ax in combination with an LW-500), a profile error occurs and the WLAN will not be broadcast by that access point.
	Configure 5 GHz mode	Yes	If a setting for the 2.4 GHz band is selected but is not supported by the access point (e.g. 802.11ax in combination with an LW-500), a profile error occurs and the WLAN will not be broadcast by that access point.
	Configure 5 GHz sub-bands	Yes	
	Set DTIM period	No	The DTIM period in LCOS LX is fixed at 1.
	Set the background scan interval	No	
	Set antenna gain	Yes	
	Set TX power reduction	Yes	LCOS LX always calculates the reduction based on a transmission power of 30 dB. This results in the following constellations for the various frequency bands and the sub-bands in the 5 GHz band: › **2.4 GHz with 20 dB permitted transmission power:** Implementing a transmission power reduction of 10 dB requires a value of 20 dB to be entered. › **5 GHz sub-band 1 with 23 dB permitted transmission power:** Implementing a transmission power reduction of 3 dB requires a value of 10 dB to be entered. › **5 GHz sub-band 2 with 30 dB permitted transmission power:** In this case, no conversion is required. Entering a value of 5 dB also results in a 5 dB reduction in transmission power.
	To activate the VLAN module	–	Activating the VLAN module in LCOS LX is not necessary and has no effect.
	ARC: Client steering	Yes	LCOS LX only supports **AP-based band steering**. Using the options **Yes** and **Client management** in

Area	Feature	Supported?	Remarks
			LCOS LX activates the **AP-based band steering**.
	ARC: Adaptive RF Optimization	No	
	Enable QoS according to 802.11e (WME)	Activated permanently	
	Indoor-only mode activated	Yes	
	Report seen unknown clients	No	
WLAN Controller > **Profiles** > **Advanced profiles**	Device LED profiles	Yes	
	AutoWDS	No	
	LBS server	No	
	Wireless ePaper	No	
	Wireless IDS	No	
WLAN Controller > **AP update**	Firmware management	Yes	
	Script management	No	
WLAN Controller > **Stations/LEPS**	LEPS-U	Yes	
	LEPS-MAC	Yes	
Other	ARC: RF optimization	No	
	Configuration delay (WLAN profiles)	No	
	Source address (RADIUS profiles)	No	
	IP parameter profile (AP configuration)	Yes	
	Antenna grouping (AP configuration)	No	

4.5.7 Firewall

The firewall can be used to filter traffic to and from WLAN networks at the IP level. A deny-all strategy (all traffic is blocked except for configured exceptions) or an allow-all strategy (all traffic is allowed, and only exceptions are blocked) can be used. In addition to IP addresses, hostnames / DNS names can also be used as destinations. To do this, the firewall monitors all DNS requests from clients in the affected WLAN and stores the resolved IP addresses in an internal cache until the TTL (time-to-live) expires. If a client subsequently attempts to establish a connection to an IP address identified in this way, the connection can be blocked or allowed, depending on the configuration.

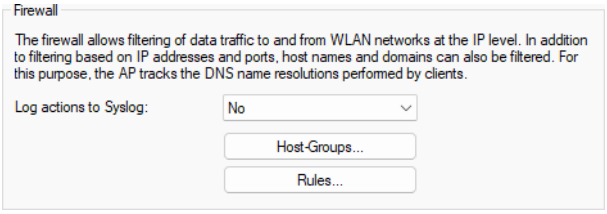
Monitoring DNS requests is only possible with unencrypted DNS. If the client uses encrypted methods such as DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS), the DNS requests cannot be inspected. In this case, it may be advisable to block these DNS methods using the firewall as well. DoT can be blocked by blocking the port used for it, port 853. DoH uses the regular HTTPS port 443 and therefore cannot be blocked in general; however, DoH servers are usually initially resolved using regular DNS, so popular DoH server domains can be blocked by specifying their names in the firewall.

It is not possible to block DoH completely by design. If preventing all uncontrolled traffic is the priority, it is therefore recommended to configure a deny-all strategy and explicitly allow permitted services.

When a client roams between APs, the client's applications normally do not issue new DNS requests in response. This usually occurs only after the TTL (time-to-live) expires. The firewall of the AP to which the client has roamed therefore cannot analyze DNS requests or learn the resolved IP addresses and, as a result, cannot actually block the client's traffic. To enable this nevertheless, the firewall's DNS cache is transferred and kept synchronized via IAPP between APs configured with the same SSID or SSIDs. This causes all associated APs in the network to generate the same effective firewall rule set and filter traffic based on the IP addresses that any AP in the network has identified from the client's DNS requests. The current DNS cache can be viewed on the AP using the CLI command `ls /Status/DNS/Snooping-Results`.

Note that only the (volatile) DNS cache is synchronized. The AP configuration, consisting of host groups and filter rules, is not synchronized and must be kept identical separately for all APs.

The settings for the IP- and DNS-based firewall are available under **Wireless LAN** > **Firewall**.



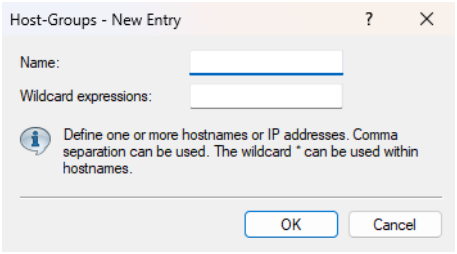
Log Actions to Syslog

When a firewall rule is processed, an entry is created in Syslog.

Depending on the amount of traffic, this may require significant CPU resources and generate a large number of Syslog messages.

4.5.7.1 Host-Groups

Configure hostnames or IP addresses here for use in the firewall rules later.



Name

Name of the group.

Wildcard expressions

One or more comma-separated IP addresses or hostnames. You can use the wildcard character * in this field to represent any characters.

The syntax of the wildcard expressions is compatible with that of the app definitions for LCOS.

4.5.7.2 Rules

Configure the firewall rules here.

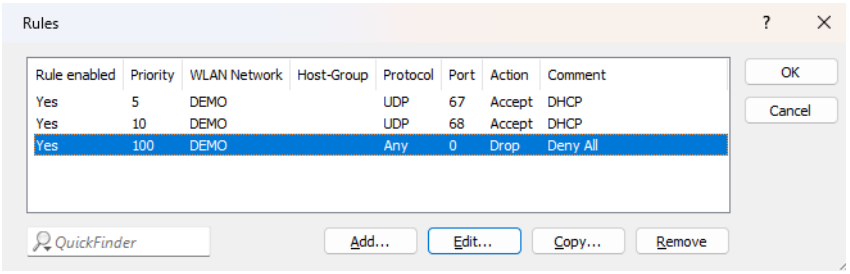
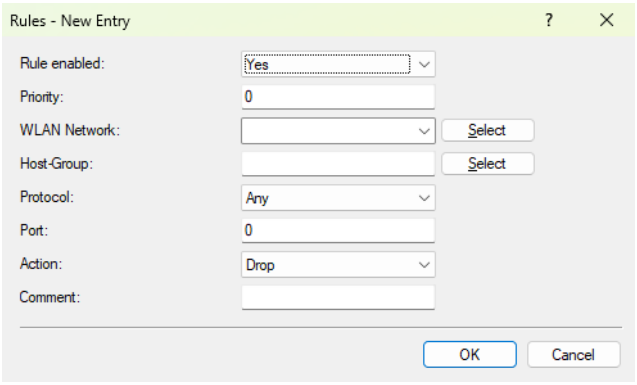


Figure 1: Deny-All Example

Note that the deny-all rule blocks **all** traffic. Therefore, you must explicitly allow the appropriate ports for DHCPv4 to enable IPv4 address assignment.



Rule enabled

Specifies whether the rule is active for the firewall.

Priority

Priority of the rule. Rules with lower values are processed before rules with higher values.

WLAN Network

The WLAN network for which the rule is active.

Host-Group

One or more previously configured host groups against which the destination of the rule is checked.

Protocol

Configures whether the rule applies only to TCP, UDP, or all traffic.

Port

If TCP or UDP is entered as the protocol, you can additionally specify a port number here as a filter criterion.

Action

Configures whether the connection is allowed or discarded when the rule applies.

Comment

A free-text field for entering any comment.

4.5.8 End-to-End Test

The WLAN end-to-end test can be used to check the availability and performance of a WLAN from the perspective of an end device—without requiring an additional test device on site. To do this, an existing R&S®LANCOM access point is temporarily switched to client mode and performs defined tests along the entire connection path from the WLAN to the Internet.

The test detects, among other things, problems with WLAN authentication, IP address assignment via DHCP, name resolution via DNS, logging in to a captive portal, and ping and HTTP connections. Test profiles can be adapted to the respective network environment. Tests that are not required can be removed from the profile, such as the captive portal test if no hotspot is operated.

An administrator can start a test run manually when required or schedule it regularly using the internal cron table. The results are stored in the corresponding log tables and are also forwarded to the device Syslog. From there, they can be forwarded, for example, to external SIEM systems.

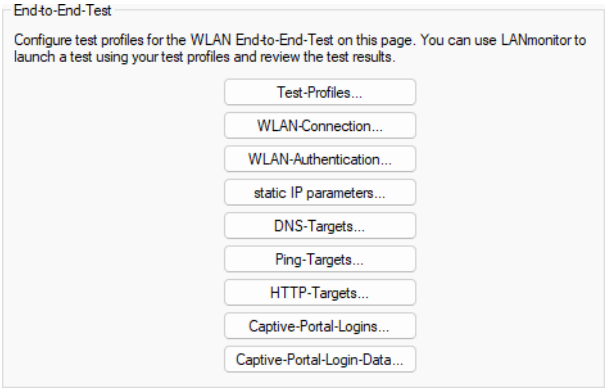
During test execution, the access point operates in client mode. As a result, it is temporarily unavailable for normal WLAN operation, and connected clients are disconnected. After the test run is complete, the access point automatically switches back to normal operating mode and resumes serving the WLAN clients.

The tests are executed in a defined order:

1. WLAN connection
2. Network connection, including DHCPv4, DHCPv6, and SLAAC
3. DNS resolution
4. Captive portal
5. Ping
6. HTTP connection

This order cannot be changed because the individual tests build on one another. For example, a WLAN connection is required for network communication, a valid IP address is required for DNS queries, and an HTTP test may be possible only after successfully logging in to the captive portal.

The settings for the WLAN end-to-end test are available under **Wireless-LAN** > **End-to-End Test**.



Test Results

The results of the individual subtests are stored in separate tables under **Status** > **WLAN** > **End2End-Test**. In addition, there is a separate history table that lists the results of all subtests chronologically in a single table. The history table is therefore comparable to a Syslog, but contains only entries for the WLAN E2E test.

4.5.8.1 Test Profiles

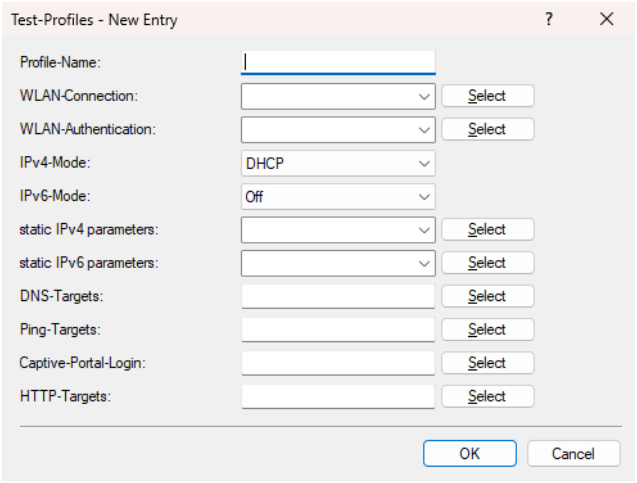
This menu is used to compile test runs. A test run consists of multiple individual tests that are executed together.

At least one test in the **WLAN-Connection** category must be configured for each test profile. Additional individual tests can be added optionally, depending on which tests are to be performed.

If **WLAN-Authentication** is left empty, an open WLAN connection without encryption is used. In this case, the SSID must provide an open network.

Static IPv4 or IPv6 parameters can be left empty if no static parameters were selected in the respective **IPvX-Mode**.

Multiple individual tests of the same category can be executed per test profile. To do this, specify the corresponding tests separated by commas.



Profile-Name

The name of this test profile.

WLAN-Connection

Select one of the available WLAN connections.

WLAN-Authentication

Select one of the available WLAN authentication configurations.

IPv4-Mode

Select either DHCP or Static.

IPv6-Mode

Select either Router Advertisement, DHCPv6, Static, or Off.

static IPv4 parameters

If required, select the static IPv4 parameters.

static IPv6 parameters

If required, select the static IPv6 parameters.

DNS-Targets

Select one of the available DNS targets.

Ping-Targets

Select one of the available ping targets.

Captive-Portal-Login

Select one of the available captive portal logins.

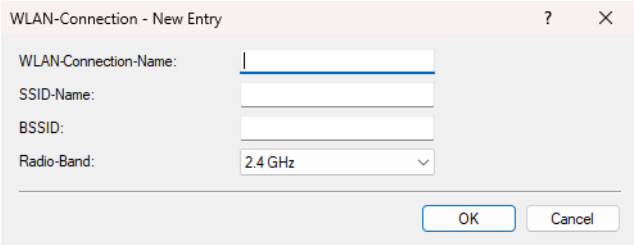
HTTP-Targets

Select one of the available HTTP targets.

4.5.8.2 WLAN Connection

Specify the SSID to which the connection is established and on which the tests are performed.

Optionally, you can specify a particular BSSID if the connection should be established to a specific access point. If no BSSID is configured, the test automatically selects an access point with the specified SSID. The access point with the strongest signal is preferred.



WLAN-Connection-Name

Enter a name for this connection.

SSID-Name

The SSID for the tests.

BSSID

Optional BSSID for the tests.

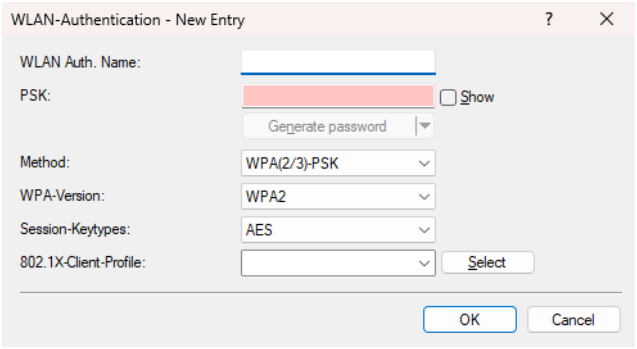
Radio-Band

The radio band for this connection.

4.5.8.3 WLAN Authentication

The WLAN E2E test supports both PSK authentication and IEEE 802.1X authentication with the usual client-side options.

To use IEEE 802.1X, you must first configure a suitable supplicant profile.



WLAN-Auth.-Name

Enter a name for this WLAN authentication configuration.

PSK

Enter the PSK.

Method

Select the WLAN authentication method.

WPA-Version

Select the WPA version.

Session-Keytypes

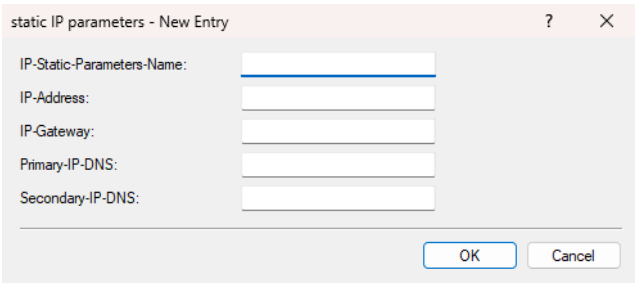
Select the session key type.

802.1X-Client-Profile

Select an IEEE 802.1X client profile.

4.5.8.4 Static IP parameters

If a static IP configuration is to be used for the test, enter the corresponding IP parameters in this table.



IP-Static-Parameters-Name

Enter a name for this static IP configuration.

IP-Address

Enter the IP address.

IP-Gateway

Enter the IP gateway.

Primary-IP-DNS

Enter the IP address of the primary DNS server.

Secondary-IP-DNS

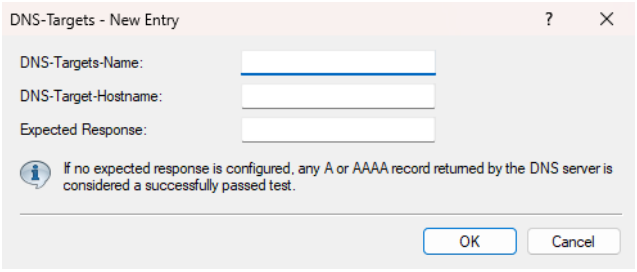
Enter the IP address of the secondary DNS server.

4.5.8.5 DNS Targets

Configure the DNS test here. In the **Expected Response** field, you can use the prefix “A:” or “AAAA:” to specify that a particular A or AAAA record is expected.

You can specify multiple records as a comma-separated list. The test is considered successful as soon as one of the configured records matches the received response.

If the **Expected Response** field is left empty, any received A or AAAA record is considered a successful response.



DNS-Targets-Name

Enter a name for this DNS target.

DNS-Targets-Hostname

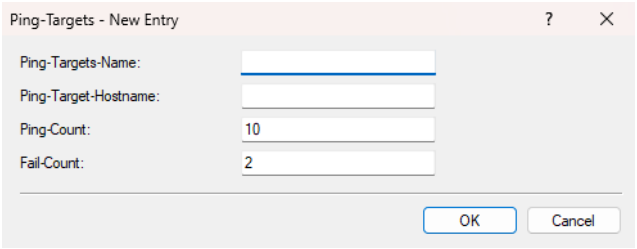
Enter the hostnames to be tested.

Expected Response

Enter the response expected for this test.

4.5.8.6 Ping Targets

Configure the ping/ICMP test here. The Ping Count and Failure Count fields are prepopulated with the displayed default values and can be adjusted as needed.



Ping-Targets-Name

Enter a name for this ping target.

Ping-Targets-Hostname

Enter the hostname to be tested.

Ping-Count

Enter the number of pings.

Failure-Count

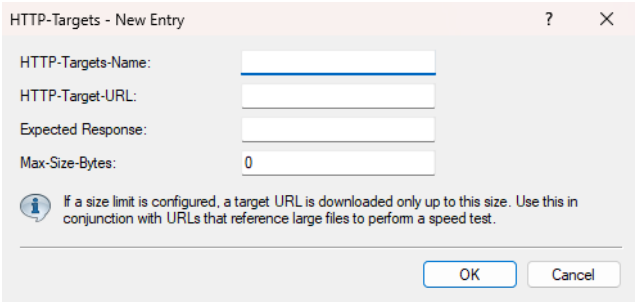
Enter the number of failures.

4.5.8.7 HTTP Targets

You can test an HTTP connection in this table. The E2E test accesses the configured **HTTP-Target-URL** and compares the received HTTP status code with the value specified in the **Expected Response** field.

The HTTP test can also be used as a speed test if a sufficiently large file can be downloaded from the HTTP target URL. To enable a meaningful throughput measurement, **Max-Size-Bytes** should also be configured in this case. If no maximum value is specified, the entire file is downloaded.

The measured throughput is always displayed in the test results. However, this value is meaningful only if a sufficiently large file is downloaded and the TCP/HTTP download can reach a realistic transfer speed.



HTTP-Targets-Name

Enter a name for this HTTP target.

HTTP-Target-URL

Enter the URL to be tested.

Expected Response

Enter the expected response.

Max-Size-Bytes

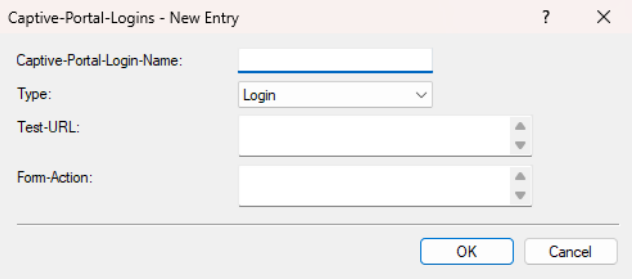
Optional size limit.

4.5.8.8 Captive Portal Logins

If the network being tested is protected by a captive portal, you can configure the required login parameters here.

The E2E test first accesses the configured test URL to check whether the captive portal redirects the request. If a redirect is detected, the test creates an HTTP POST request with the entries from the Captive Portal Login Data table and sends it to the URL specified in the Form Action field.

The test URL is then accessed again. If no redirect occurs, the login is considered successful and the test passes.



Captive-Portal-Login-Name

Enter a name for this captive portal login.

Type

You can select either “Login” or “Logout” here.

Depending on the captive portal, it may be useful to log the user out again after the test is completed. This can, for example, conserve resources on the captive portal gateway or allow the same credentials to be used for subsequent test runs.

To do this, create an additional entry with the type “Logout”. Configure the **Form Action** so that it performs the logout action of the captive portal. The logout URL may differ from the URL of the login form. Analyze the HTML code of the respective portal for this purpose.

However, many modern captive portals with click-through login do not provide a logout function. In this case, the user session is terminated only after a timeout. A captive portal test that runs regularly at short intervals may then succeed without actually checking the login, because the MAC address of the testing access point is still cached in the captive portal.

If you manage the captive portal yourself, a special test function may be useful. For example, a hidden form in the HTML code could start a dedicated test session that automatically expires after a short time.

Test-URL

This is the URL that the E2E test accesses to determine whether the captive portal redirects the request. It can point to any URL that reliably responds with an HTTP status code in the “200” range. Ideally, use a URL that responds with “200” or “204”.

This field is empty by default because no URL from an external third party can be specified as a fixed default. Therefore, you must configure a suitable URL.

Form-Action

This is the URL to which the login credentials are transmitted via HTTP POST. For a classic LCOS Public Spot, this could be a URL such as the following:

```
https://pspot.lancom.de:443/authen/login/
```

If this field remains empty, the E2E test automatically uses the URL to which the captive portal redirected the request when the Success URL was accessed for the first time. For R&S®LANCOM Management Cloud-based hotspots, this usually enables login without additional configuration of this URL.

4.5.8.9 Captive Portal Login Data

This table is used to configure the form elements that are transmitted to the captive portal via HTTP POST for logging in or logging out.

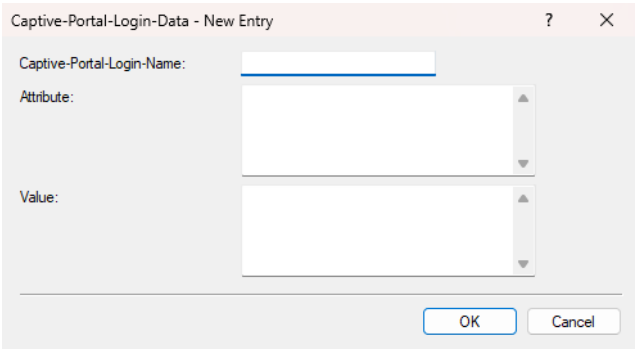
For a classic Public Spot based on LCOS, the form data could look as follows:

Attribute	Value
AGB	checked
password	secret
userid	rsnc

If the logout function is also used, the corresponding attributes for the logout test must also be stored in this table.

Each captive portal uses its own form structure. Therefore, use the portal's HTML source code to determine the correct form and the required attributes and values.

For very simple portal pages that contain only a single form attribute, such as a button for click-through login, the E2E test attempts to transmit this attribute automatically via POST. In this case, no additional configuration in this table is required. This currently works, for example, with the One-Button login of the R&S®LANCOM Management Cloud hotspot.



Captive-Portal-Login-Name

Enter a name for this captive portal login.

Attribute

Enter the required attributes here.

Value

Enter the values for the configured attributes here.

4.6 IoT – the Internet of Things

Here you will find the settings for IoT technologies supported by LCOS LX, such as Wireless ePaper and Bluetooth Low Energy.

IoT networks interconnect physical and virtual objects to facilitate the exchange of data and information. Typical examples include sensors, smart home appliances, digital room signs, and electronic shelf labels. IoT devices are largely networked by radio, using a variety of wireless technologies such as modified ZigBee variants (retail IoT), Bluetooth Low Energy (BLE), or the

various cellular offshoots. There is no uniform “IoT wireless standard”, and new IoT radio technologies are emerging in rapid cycles.

The specific settings for IoT are made in LANconfig under **IoT**.

4.6.1 Wireless ePaper

R&S®NC Wireless ePaper Displays provide a variety of options for displaying information. You can automatically and remotely update the calendar schedule for your conference rooms, you can create dynamic notices and direction signs, or you can control the price labels of goods on your shelves from a central location in real time. The wide range of different settings allows you to set up your very own customized use case.

The settings for operating Wireless ePaper Displays are to be found in LANconfig under **Tools** > **Options** > **Wireless ePaper**. Under IP/hostname you enter the IP address and the port of the Wireless ePaper Server. The recommended port number is 8001.

You invoke the Wireless ePaper management in LANconfig under **Tools** > **Start Wireless ePaper management**.

4.6.1.1 Settings for Wireless ePaper

Wireless ePaper Displays from LANCOM offer state-of-the-art digital signage for a wide range of applications. The Displays are controlled by an innovative wireless technology with extremely low power consumption.

ePaper operations require the use of a USB-connected R&S®NC Wireless ePaper USB expansion module for each device.

Activate the Wireless ePaper radio module in LANconfig under **IoT** > **Wireless ePaper** > **Wireless ePaper**.



Operating

Use this to activate the Wireless ePaper feature in the access point.

The server must be configured for the connection type ThinAP2.0/TCP. Please refer to the *R&S®NC Support Knowledge Base* for further information. Use the same method to set the following two configuration options to enable communication between the server and LCOS LX access points:

```
accessPointUseThinMode?value=true accessPointThinUseOutboundMode?value=true
```

This can be done, for example, with “curl” as follows:

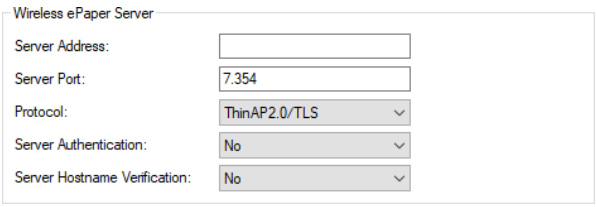
```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true

curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

The legacy connection mode via UDP is not supported by LCOS LX.

Wireless ePaper Server

Activate the Wireless ePaper Server in LANconfig under **IoT** > **Wireless ePaper** > **Wireless ePaper Server**.



Server address

Here you configure the IP address of the Wireless ePaper Server that the access point should contact.

Server port

The TCP destination port to be used for communication with the server.

Protocol

The protocol used to communicate with the server.

Server Authentication

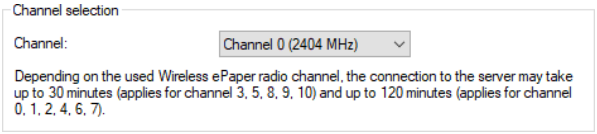
Optionally, the access point can check the server certificate of the Wireless ePaper Server when it connects to it. If this option is enabled, a corresponding CA certificate (or certificate chain) in PEM format must also be loaded onto the access point via WEBconfig.

Server Hostname Verification

In connection with the **Server Authentication** option, this setting decides whether the “Common Name” specified in the certificate is checked for a match with the host name of the addressed Wireless ePaper Server.

Channel selection

Activate the channel used by the Wireless ePaper Server in LANconfig under **IoT** > **Wireless ePaper** > **Channel selection**.

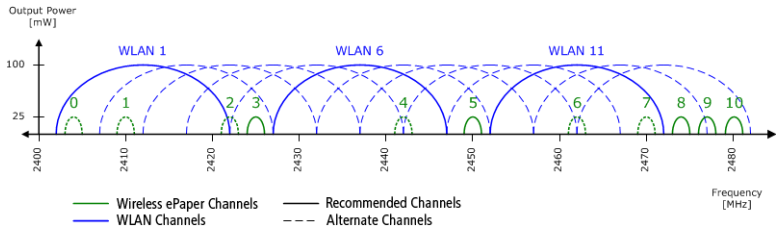


Channel

Configure the radio channel to be used for controlling the Wireless ePaper Displays.

Depending on the radio channel used, connecting the server to a Display can take up to 30 minutes (channels 3, 5, 8, 9, 10) or up to 120 minutes (channels 0, 1, 2, 4, 6, 7). If possible, you should prefer the channels 3, 5, 8, 9 and 10, as Wireless

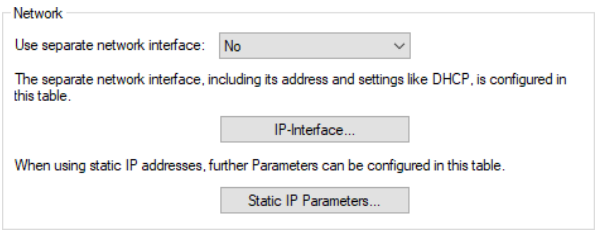
ePaper Displays scan them more frequently and they do not interfere with the popular Wi-Fi channels 1, 6, and 11.



Do not select the same channel for two access points that are in the same area. This causes interference and prevents Displays from joining the network. It is possible to set the same channel on two access points if you are sure that each display is only within range of one of these access points.

Network

Configure an optional separate network interface of the Wireless ePaper Server in LANconfig under **IoT** > **Wireless ePaper** > **Network**.This function allows you to specify a separate IP/VLAN interface for the access point's Wireless ePaper client. This means that the connection to the ePaper server or the Vusion Cloud can be established via a separate interface from the standard management IP/VLAN interface.

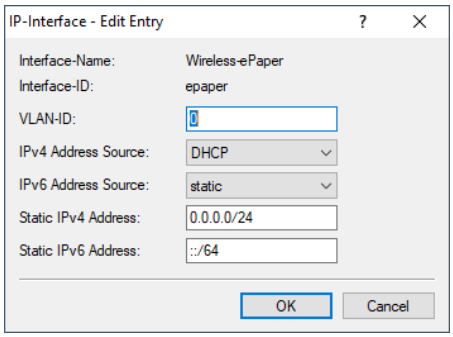


Use separate network interface

Activate a separate interface for the connection to the ePaper server or the Vusion Cloud.

IP interface

Configure the separate IP interface for the connection to the ePaper server or the Vusion Cloud.



Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

Interface-ID

The internal identifier for the interface.

VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible. The default value “0” means that no VLAN is used.

IPv4 address source

Here you select how the IPv4 address of the interface is to be obtained.

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

IPv6 address source

Here you select how the IPv6 address of the interface is to be obtained:

Router-Advertisement

The IPv6 address is derived from router advertisements that the device receives on the respective interface.

If the flag in the router advertisement is set to Other and/or Managed, additional configuration options are obtained via DHCPv6—even if the address source is set to **Router-Advertisement**.

DHCPv6

The IPv6 address is obtained via DHCPv6.

Static

The static IPv6 address configured for the interface is used.

Static IPv4 address

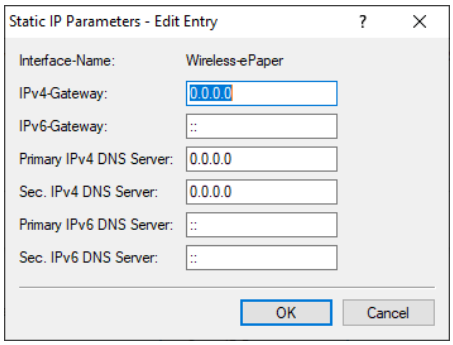
Here you configure the IP address to be used when the IPv4-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. “/24”) as a suffix.

Static IPv6 address

Here you configure the IP address to be used when the IPv6-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. “/64”) as a suffix.

Static IP Parameters

Here you configure the IP and network settings that apply when you use static IP addresses.



The settings made in this table only come into effect if the IPv4 or IPv6 address source for the IP interface is set to **static**. Otherwise all of the necessary information is retrieved via DHCP, for example, in which case no configuration is required here.

Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Primary IPv4 DNS server

Here you configure the primary IPv4 DNS gateway for the referenced interface.

Secondary IPv4 DNS server

Here you configure the secondary IPv4 DNS gateway for the referenced interface.

Primary IPv6 DNS server

Here you configure the primary IPv6 DNS gateway for the referenced interface.

Secondary IPv6 DNS server

Here you configure the secondary IPv6 DNS gateway for the referenced interface.

4.6.2 Bluetooth Low Energy (BLE)

The settings for Bluetooth Low Energy are located here.

The specific settings for BLE are made in LANconfig under **IoT** > **Bluetooth LE**.



Operation

By turning on the BLE radio here, data about the BLE environment is collected continuously.

BLE Scan Type

Choose between a passive and an active scan. The BLE name and a scan response can only be detected in the active scan. Note that BLE clients answering scan requests can increase power consumption.

4.6.3 USB

Here you will find the settings for USB Ethernet support. Selected USB Ethernet devices are supported on access points with USB port. The CDC-EEM protocol is used here. For this purpose, the USB Ethernet device is hybridized with the LAN of the access point. It is possible to specify a VLAN ID for network segmentation. Therefore, make sure that the USB Ethernet device can communicate in your network and, if necessary, VLAN according to the manufacturer's specifications. The following USB Ethernet devices are qualified for operation with LCOS LX-based access points:

- Hanshow HS_C09978 ESL Controller
- SoluM EGU200NA0X ESL GEN2 USB Gateway

The special settings for USB Ethernet support are made in LANconfig under **IoT** > **USB**.



Operating

Switch on the USB Ethernet support here.

VLAN ID

Optional specification of a VLAN ID.

4.7 Other services

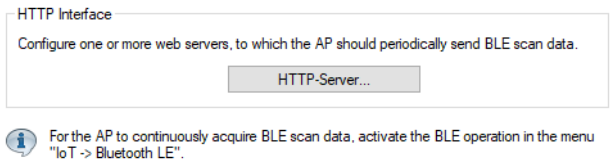
This item contains the settings for services supported by the LCOS LX, such as Location Based Services.

4.7.1 Location-based services (LBS)

R&S®NC access points are able to work as LBS clients with an LBS server. In this case, they report any BLE clients within range to the LBS server, which can then offer location-based services to those clients. As of LCOS LX 5.30, an HTTP interface is supported.

Using the HTTP interface, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

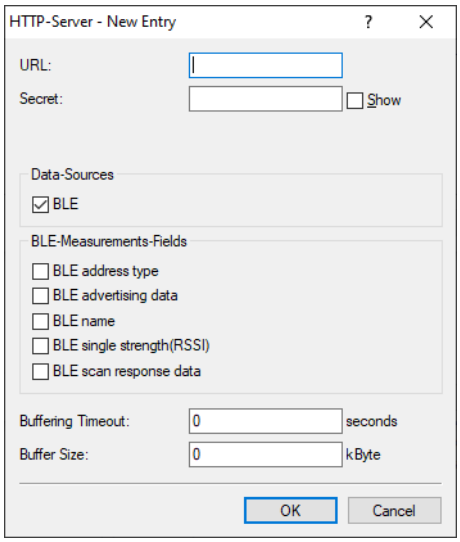
LANconfig: **Miscellaneous Services** > **Location Based Services**



In order for the access point to collect BLE data, the BLE feature has to be switched on separately. Please refer to *Bluetooth Low Energy (BLE)* on page 114 or *Location based services* on page 157.

4.7.1.1 HTTP-Server

Under **HTTP-Server** you configure the HTTP endpoints for the LBS data.



URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. This can be done using WEBconfig. See *Location based services* on page 157.

Secret

The secret (key) is transmitted from the access point to the end point in the JSON messages and can additionally be used for message authentication.

Data-Sources

Here you configure the types of LBS data that should be sent. Only BLE is currently available.

BLE-Measurements-Fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.

Buffering Timeout

After the configured time (in seconds) is reached, all BLE messages buffered up to that point are sent to the server.

Buffer Size

After the configured data quantity (in bytes) is reached, all BLE messages buffered up to that point are sent to the server.

With the value for **Buffering Timeout** and **Buffer Size** both set to 0, the messages are sent to the server as soon as possible.

Data format of the messages sent to the endpoint

› For **BLE**:

```
{
    "deviceMac": "00A0574C49EB",
    "measurements": [
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076493
        },
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076494
            "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
            "scanResponseData": "050974657374"
        }
    ],
    "secret": "",
    "type": "BLE",
    "version": "1.0"
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the access point configuration.

type

The type of data sent. Can be either WLAN or BLE.

deviceMac

The LAN MAC address of the access point.

measurements

This contains at least one measured value. This could also be a number of measurements.

deviceAddress

The address of the BLE device or client.

seenTime

The time stamp (in Unix time) when the BLE frame from the client was received by the access point.

addressType

The type of BLE address. The following address types are available: `Public` or `Random`.

rssi

The signal strength in dBm of the received BLE frame.

name

The name submitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

advertisingData

The complete advertisement transmitted by the BLE device.

scanResponseData

The complete scan response transmitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

5 Configuring features with WEBconfig

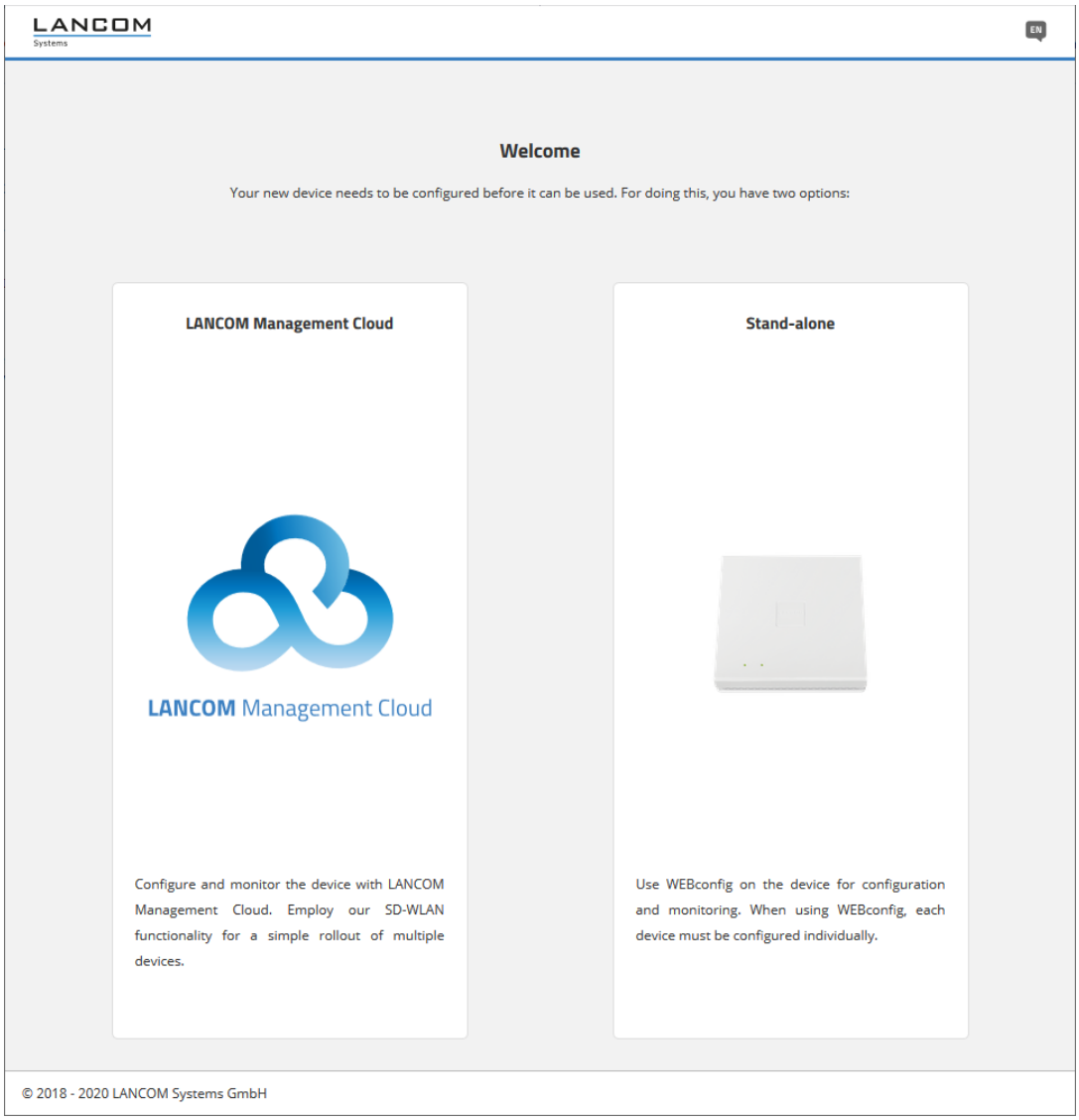
The following section explains how devices are installed with WEBconfig and the various settings that WEBconfig has to offer. These depend on the device, so not all of the listed options are available with every device.

5.1 Commissioning of a device via WEBconfig

WEBconfig is reached via HTTP and HTTPS. If you use HTTP, the device automatically redirects you to an encrypted HTTPS connection.

WEBconfig uses a self-signed SSL certificate, so this must be added as an exception in the browser for each device.

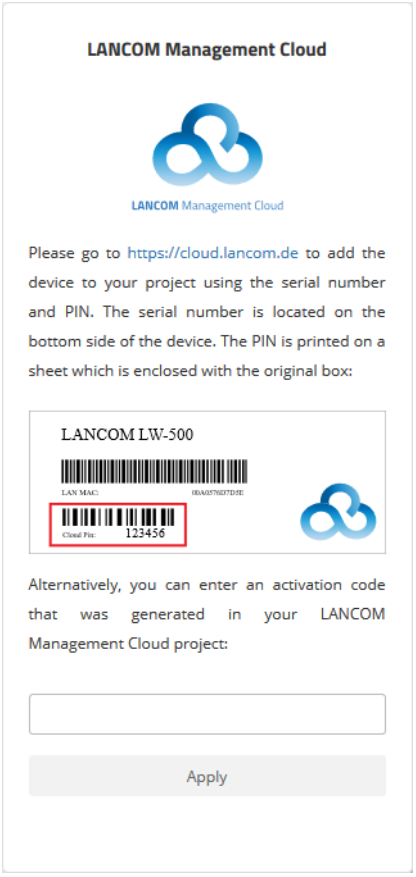
After invoking the WEBconfig interface of an unconfigured device, you can select whether the device should be managed by the R&S®LANCOM Management Cloud or as a stand-alone device.



Click the corresponding button here to decide whether the device should be managed by the R&S®LANCOM Management Cloud or as a stand-alone device.

5.1.1 Management by R&S®LANCOM Management Cloud

You either connect the device to the R&S®LANCOM Management Cloud by means of the serial number and PIN (zero touch), or you use the corresponding input field to enter an activation code that you generated previously in your R&S®LANCOM Management Cloud project:



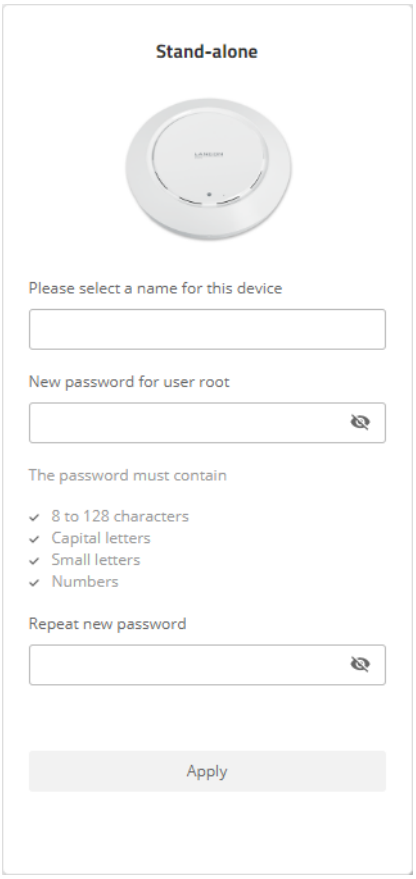
After confirming the activation code and completing the pairing process, a success message will be displayed and you will be redirected to the WEBconfig login page. The device can now be managed via the LMC.

5.1.2 Stand-alone management

Use the corresponding input fields to set a meaningful name for your device and set a password to be used by the user “root”. The password must meet the following criteria:

- at least 8 characters
- at least one letter
- at least one digit
- at least one special character

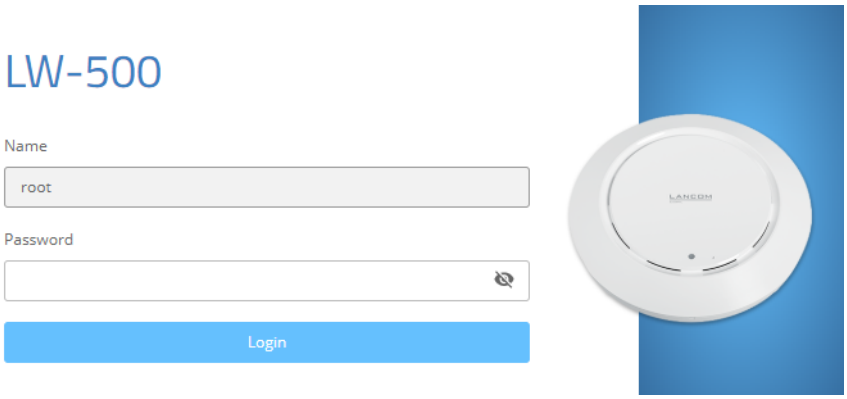
The password set here is valid for the user “root”. This user is also used subsequently to login to WEBconfig.



Clicking on **Apply** will direct you to the login page. Use the username “root” and the previously defined password to login to WEBconfig.

5.2 Login

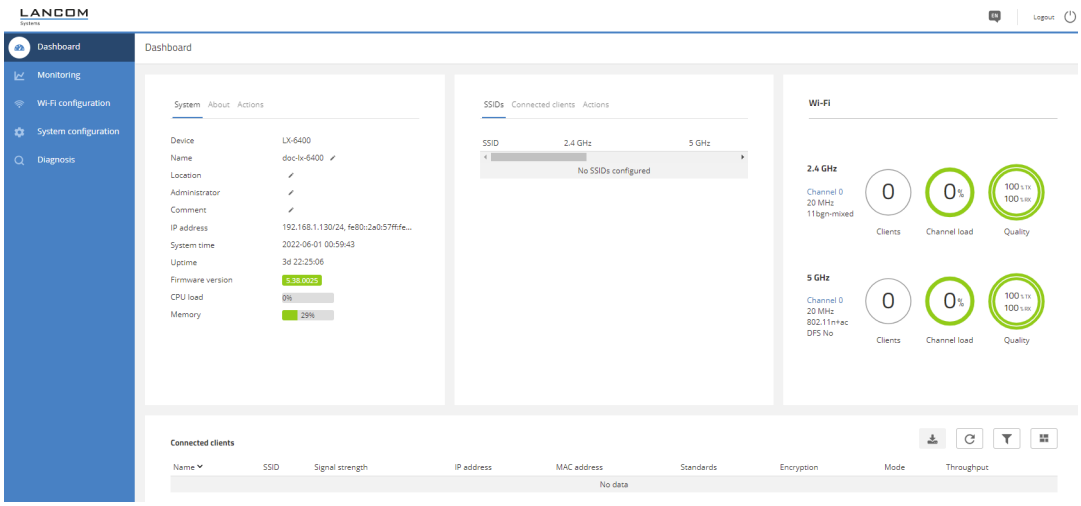
Login by entering the user name “root” and the password you set earlier:



After logging in to WEBconfig you will be taken to the dashboard. Refer to section *WEBconfig – Dashboard* on page 123 for information on the dashboard.

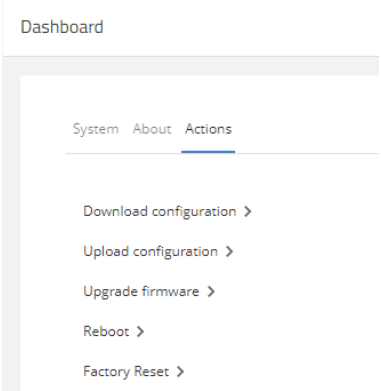
5.3 WEBconfig – Dashboard

The dashboard provides an overview of the essential operating data for your device.



5.3.1 Actions

The new features described below are located on the dashboard in the system overview under the **Actions** item.

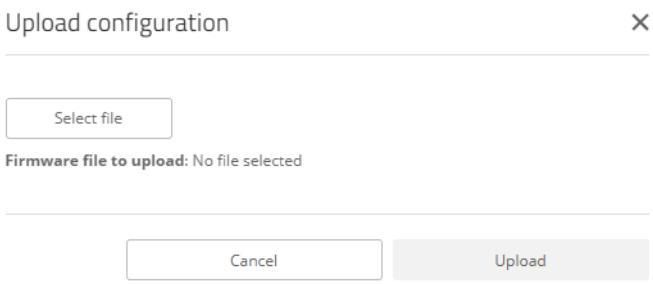


5.3.1.1 Download configuration

The action **Download configuration** lets you download a device configuration in the *.lcf format. A click on the action immediately downloads the configuration.

5.3.1.2 Uploading configuration

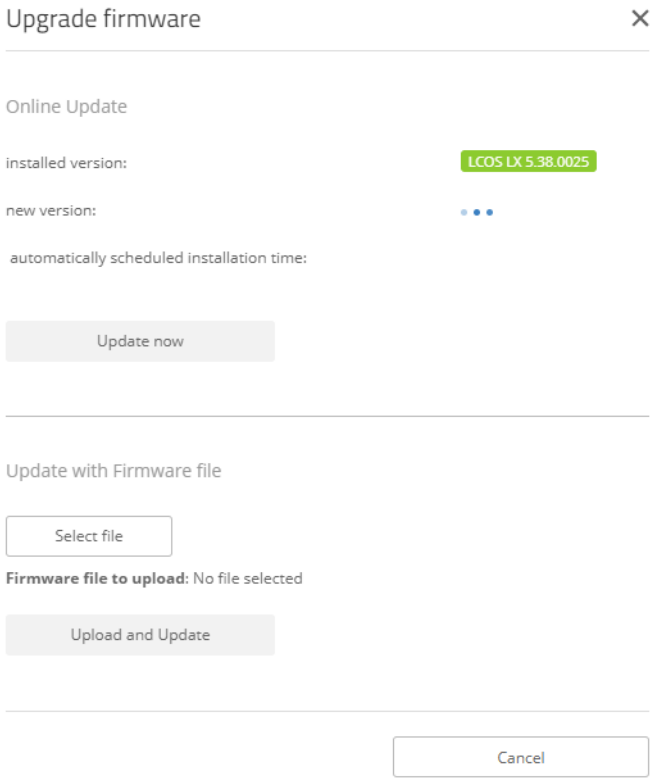
The action **Upload configuration** lets you upload a new device configuration in the *.lcf format.



Click **Select file** to select a configuration file. Use the button **Upload** to upload this file to the device.

5.3.1.3 Update firmware

Use the action **Update firmware** to upload new firmware to the device.



The items **Online Update** and **Update with Firmware File** are available.

Online Update

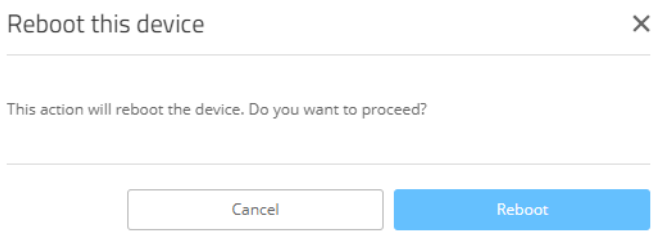
An automatic search is made for firmware that is made available online and that is newer than the installed version. If the auto-updater is enabled, the automatically scheduled installation time for this version may be displayed. Also see *Software update* on page 39 and *Automatic firmware update* on page 150. The button **Update now** allows you to update the firmware immediately.

Update with firmware file

Use **Select file** to select a firmware file that you want to upload to the device. This may also be a previous version that you want to go back to. The button **Upload and Update** uploads the selected firmware file to the device, so updating the firmware.

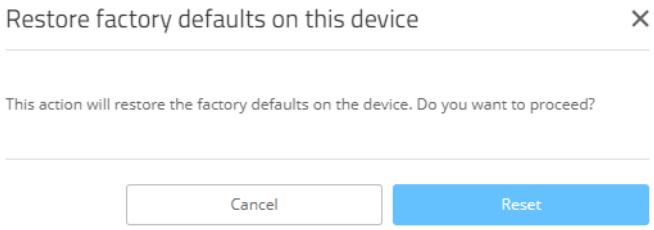
5.3.1.4 Reboot

The action **Reboot** restarts the device after a security prompt.



5.3.1.5 Factory Reset

The action **Factory Reset** returns the device to its factory settings after a security prompt.

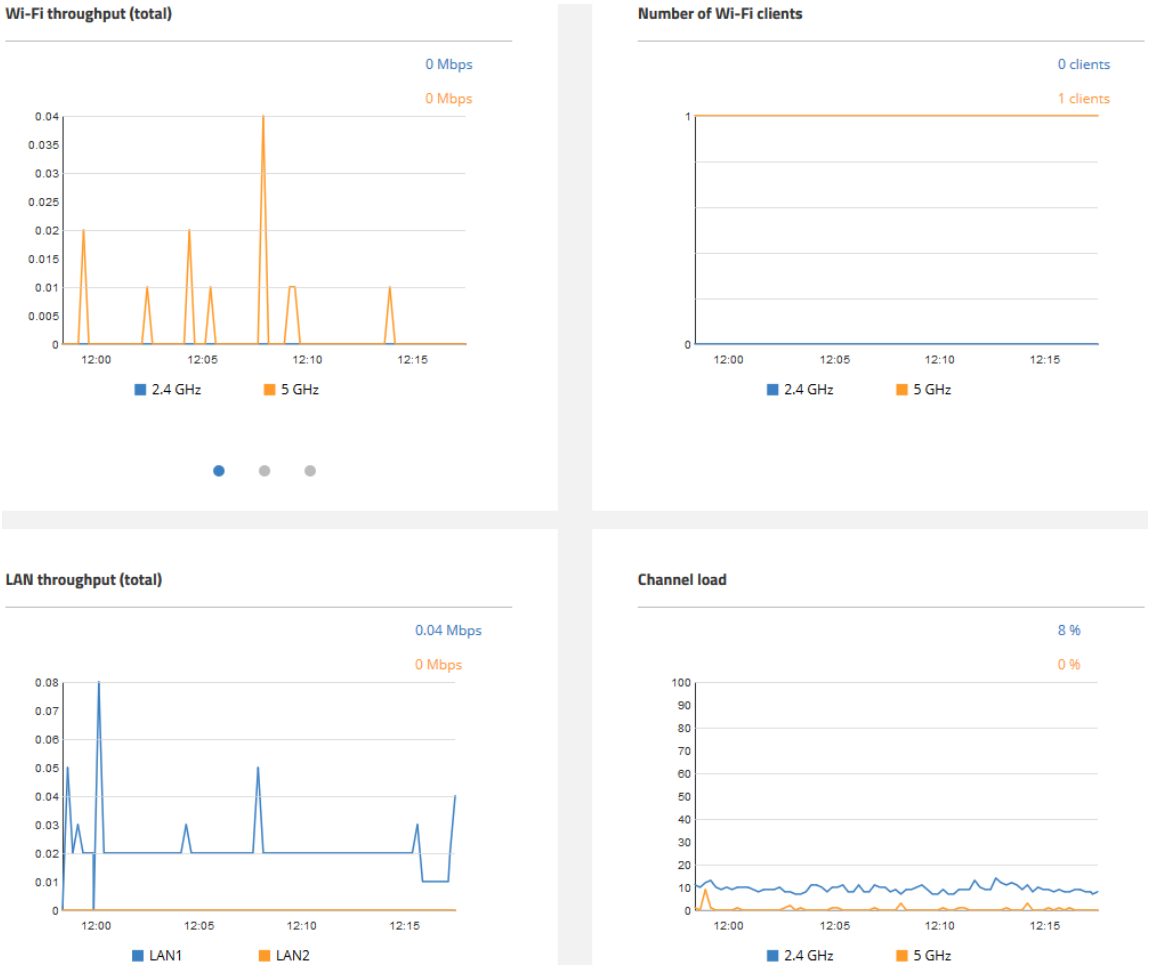


5.4 Monitoring

You reach the Monitoring area by means of the **Monitoring** item in the sidebar.

The Monitoring view is offers a graphical representation of the WLAN throughput, LAN throughput, number of WLAN stations and channel load over time.

The maximum amount of historical data available corresponds to the duration of the current WEBconfig session.



5.4.1 Neighborhood

You reach the Neighborhood area by means of the **Neighborhood** item in the sidebar.

The Neighborhood view provides an overview of the WLAN environment, especially the WLAN access points and WLAN routers that are locally active.

Click the button **Start scan** to discover the WLAN environment. After the scan is completed (duration: approx. 10 seconds), the results are shown in various diagrams and tables:



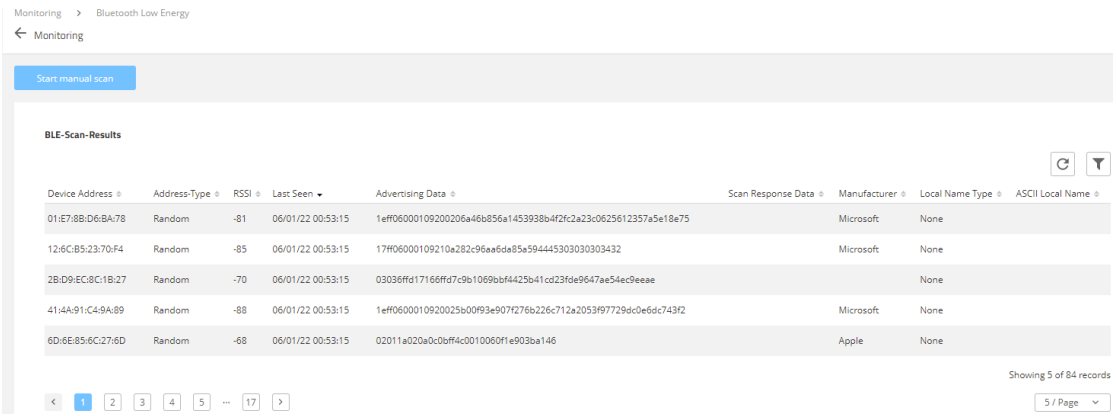
The top two bar charts visualize the number of SSIDs detected by the device on the various 2.4 GHz and 5 GHz channels, which can indicate the potential load on the channels. LANCOM access points detected by the scan and reachable on the same LAN as the current device are highlighted as “My LANCOM APs”. The WLAN channel that the current device itself is working on is also indicated. The **Neighborhood** table also provides details about the SSIDs detected by the scan, such as the name, the BSSID (MAC address), and the signal strength.

5.4.2 Bluetooth Low Energy

You reach this section by means of the **Bluetooth Low Energy** item in the sidebar.

The **BLE-Scan-Results** provide an overview of the Bluetooth environment.

Click the button **Start manual scan** to discover the BLE environment. The results are displayed after the scan is complete:



5.5 Wi-Fi configuration

You reach this area by means of the **Wi-Fi configuration** item in the sidebar.

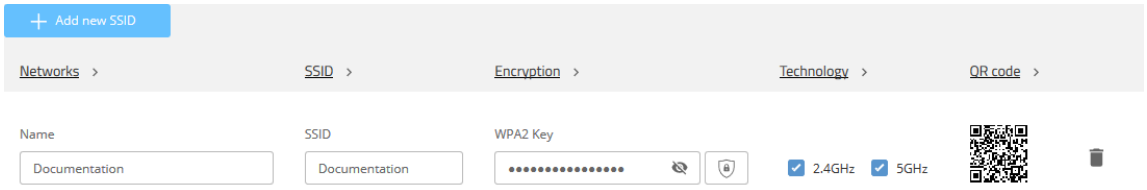


5.5.1 Concept

The Wi-Fi configuration is designed to assist the user with the most common settings and to eliminate the hassle of configuring minor details. It remains possible to configure different scenarios.

5.5.2 Operation

The available SSIDs are displayed in tabular form. Click on the **Add new SSID** button to configure a new SSID. A new line is added. To configure an SSID with WPA2-PSK, all you have to do is fill out the fields **Name**, **SSID** and **WPA2 key**.



Depending on your needs, you can generate a secure WPA2 key automatically ( ) and limit the frequency bands available for selection. By default, the SSID is broadcast on 2.4 GHz and 5 GHz.

The following restrictions must be considered when using the encryption method WEP and entering the WEP key in the field "WPA2 key":

- WEP-40-Bits / WEP-40-Bits-802.1X - Any 5 characters from the allowed set of characters OR 10 HEX characters
- WEP-104-Bits / WEP-104-Bits-802.1X - Any 13 characters from the allowed set of characters OR 26 HEX characters
- WEP-128-Bits / WEP-128-Bits-802.1X - Any 16 characters from the allowed set of characters OR 32 HEX characters

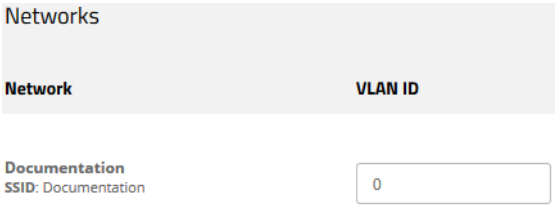
Then click on **Save** to accept your SSID. This will then be broadcast immediately by the device.

On the 5 GHz band, it may take up to a minute after the initial configuration to broadcast the SSID. This is due to a regulatory requirement to monitor the band for primary users (“radar detection” for one minute, i.e. DFS).

Further individual configuration is possible by clicking on the respective heading.

5.5.2.1 Networks

Here you can set the parameters for each SSID as follows:



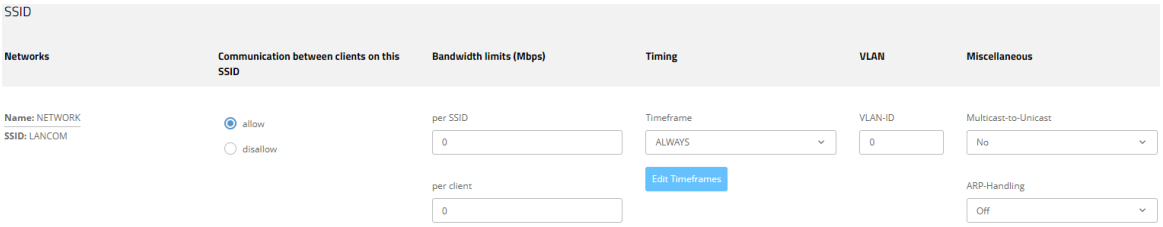
VLAN-ID

This VLAN ID is used to tag the data packets arriving from the WLAN and heading for the LAN. Similarly, packets with this VLAN ID arriving from the LAN are directed to the WLAN and are de-tagged.

> This operating mode corresponds to what is normally known as the “Access” tagging mode, since it is assumed that wireless clients usually transmit data untagged. Tagging mode cannot be adjusted.

5.5.2.2 SSID

Here you can set the parameters for each SSID as follows:



Communication between end devices on this SSID

Depending on the application, it may be desirable—or even undesirable—for clients on a WLAN network to communicate with other clients. Here you configure whether communication between the WLAN clients on the WLAN network should be allowed.

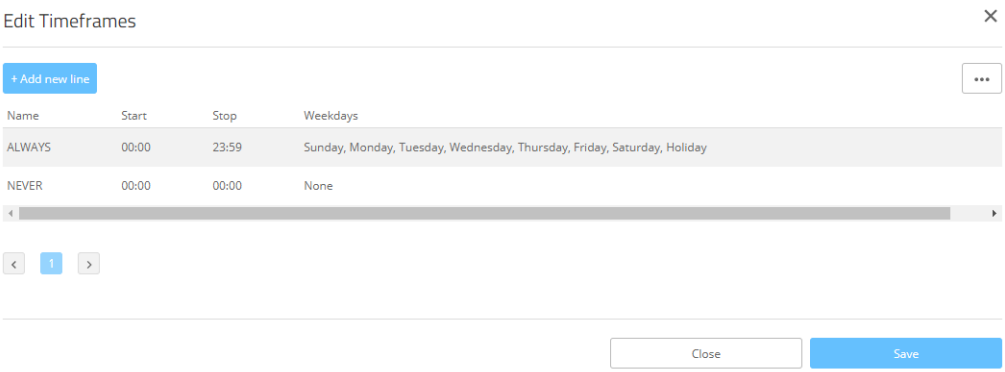
Bandwidth limits (Mbps)

Here you can limit the WLAN bandwidth used for the entire WLAN network (SSID) or limit the bandwidth available to the clients. All of the logged in clients can only send and receive data with the transmission rate configured here. The value “0” means that no limitation is active.

Timing

Timing uses time frames to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different time frames. Add the time frame here so that it is observed for this SSID.

Edit Timeframes



Name

Enter the name of the time frame so that it can be referenced from the WLAN SSID. Several entries with the same name result in a common profile. Predefined time frames are ALWAYS and NEVER.

Home

The start time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile becomes valid.

Stop

The stop time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile ceases to be valid.

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

Here you select the weekday on which the timeframe is to be valid.

Possible values:

› Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

You can form a time schedule with the same name but with different times extending over several rows.

VLAN-ID

This VLAN ID is used to tag the data packets arriving from the WLAN and heading for the LAN. Similarly, packets with this VLAN ID arriving from the LAN are directed to the WLAN and are de-tagged.

This operating mode corresponds to what is normally known as the “Access” tagging mode, since it is assumed that wireless clients usually transmit data untagged. Tagging mode cannot be adjusted.

Other

Multicast-to-Unicast

For each WLAN network, you individually configure whether and how multicasts are converted into unicasts.

No

No conversion

Convert to unicast

Multicasts are converted to unicasts (layer-2 unicast on the WLAN layer with a unicast MAC address as destination). This corresponds to the behavior in the LCOS.

Encapsulate in Unicast Aggregate

Multicasts are encapsulated in unicast aggregates (A-MSDU with unicast MAC address as destination and containing a single layer-2 multicast). This variant should be used where target applications check the destination MAC address. However, note that aggregates are not supported by 802.11a/b/g clients.

In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

ARP-Handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If “ARP handling” is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point determines the assignment between IP address and MAC address from the DHCP messages that are either exchanged between WLAN client and DHCP server or ARP requests of the connected WLAN clients are evaluated or ARP requests from the connected WLAN clients, so-called gratuitous ARP requests or ARP replies are evaluated. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to “On”.

If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to “Strict”. This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

Off

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are forwarded to the WLAN.

Strict

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are not forwarded to the WLAN.

Multicast-to-Unicast

For each WLAN network, you individually configure whether and how multicasts are converted into unicasts.

No

No conversion

Convert to unicast

Multicasts are converted to unicasts (layer-2 unicast on the WLAN layer with a unicast MAC address as destination). This corresponds to the behavior in the LCOS.

Encapsulate in Unicast Aggregate

Multicasts are encapsulated in unicast aggregates (A-MSDU with unicast MAC address as destination and containing a single layer-2 multicast). This variant should be used where target applications check the destination MAC address. However, note that aggregates are not supported by 802.11a/b/g clients.

In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

ARP-Handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If “ARP handling” is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point determines the assignment between IP address and MAC address from the DHCP messages that are either exchanged between WLAN client and DHCP server or ARP requests of the connected WLAN clients are evaluated or ARP requests from the connected WLAN clients, so-called gratuitous ARP requests or ARP replies are evaluated. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to “On”.

If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to “Strict”. This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

Off

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are forwarded to the WLAN.

Strict

ARP handling enabled. If the access point could not determine a mapping between IP address and MAC address, ARP requests are not forwarded to the WLAN.

5.5.2.3 Encryption

Here you set the encryption profile for each SSID. The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-NONE

No encryption, the SSID is open.

P-PSK-WPA2

The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

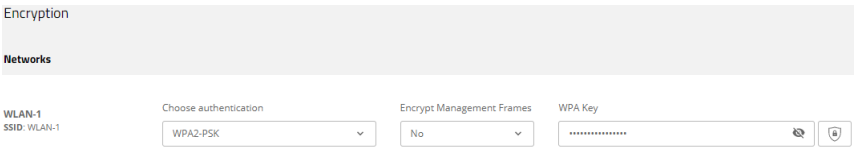
The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.

P-PSK-WiFi7

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile “P-PSK-WiFi7” is included in the configuration as of LCOS LX 7.10 and can be used.



Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

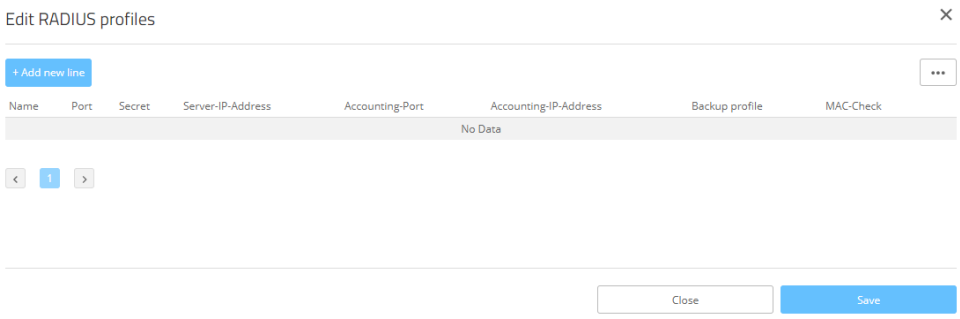
Select authentication

Change the encryption and authentication method here. WPA2-PSK (WPA2 with pre-shared key or WPA2-Personal) is preset by default. Optionally select **No encryption** or one of the following options:

- WPA3-PSK – WPA3 with pre-shared key or WPA3-Personal
- WPA(2+3)-PSK – WPA2 and/or WPA3 with pre-shared key
- WPA2-801.1X– WPA2 with 802.1X or WPA2-Enterprise
- WPA3-801.1X– WPA3 with 802.1X or WPA3-Enterprise
- WPA(2+3)-801.1X– WPA2 and/or WPA3 with 802.1X

When using methods requiring a pre-shared key (PSK), you need to enter a **WPA key**. You can read the key by clicking on the crossed-out eye symbol. Depending on your needs, you can automatically generate a secure WPA key ( ).

In the case of 802.1X you have to create a RADIUS profile. To do this, click on **Edit RADIUS profile** and add a new line there.



Name

Choose a meaningful name for the RADIUS server profile here. This internal identifier is used to reference the RADIUS server profile from other parts of the configuration.

Port

Select the port (UDP) used to contact the RADIUS server.

This is usually the port 1812 (RADIUS authentication).

Secret

Here you configure the secret used to encrypt the traffic between the device and the RADIUS server. This secret must also be stored on the RADIUS server.

Server IP address

Here you configure the host name or IP address where the RADIUS server is to be reached.

Accounting port

Select the port (UDP) used to contact the RADIUS accounting server.

This is usually the port 1813 (RADIUS accounting).

Accounting IP address

Here you configure the host name or IP address where the RADIUS accounting server is to be reached.

Backup profile

Here you configure a backup profile, which will be used if the RADIUS server in the profile configured here cannot be reached.

MAC check

A user name can be authenticated with a MAC address instead of using the RADIUS server.

Please note that the RADIUS server generally has to be notified about the RADIUS client by means of an entry in its configuration.

Store your changes by clicking on **Save.**

Roaming

Settings for switching a client from one access point to another access point that broadcasts the same SSID.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use Opportunistic Key Caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard. See also *Fast roaming* on page 16.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Standard+Fast-Roaming

A combination of standard behavior and Fast Roaming.

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

OKC (Opportunistic Key Caching)

This option enables or disables the opportunistic key caching (OKC).

The authentication of WLAN clients via EAP and 802.1X is now standard in company networks, and for public Internet access, too, it is part of the Hotspot 2.0 specification. The disadvantage of authentication via 802.1X is the noticeably longer time between authenticating and connecting due to the exchange of up to twelve data packets between the WLAN client and access point. This may not matter for most applications that only involve exchanging data. However, time-critical applications such as Voice-over-IP rely on fast authentication when moving between WLAN radio cells so as not to impair communications.

Various authentication strategies have been established to counteract this, including PMK caching and pre-authentication, although pre-authentication by no means solves all of the problems. For one thing, there is no guarantee that the WLAN client can detect whether the access point is capable of pre-authentication. Also, pre-authentication causes a

considerable load on the RADIUS server, because it has to process the authentications of all clients and all access points on the WLAN network.

With opportunistic key caching, the management of WLAN client keys is moved to a WLAN controller (WLC) or central switch, which manages all of the access points in the network. When a client authenticates at an access point, the downstream WLC, which acts as the authenticator, performs the key management and returns the PMK to the access point for forwarding to the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID, and it sends this to the new access point in the expectation that OKC is enabled (i.e. “opportunistic”). If the access point is unable to handle the PMKID, it negotiates a regular 802.1X authentication with the client.

A R&S®NC access point is even able to perform OKC if the WLC is temporarily unavailable. In this case it stores the PMK and sends it to the WLC, once available again. The WLC then sends the PMK to all of the access points in the network so that the client can continue to use OKC when moving between cells.

In networks managed from the R&S®LANCOM Management Cloud (LMC) or networks from standalone access points, the PMKs are transmitted via the IAPP protocol. In LMC-managed networks, the IAPP is configured automatically. In networks made up with standalone access points, you have to ensure that the PMK-IAPP secret is configured and identical on every access point in the network.

IAPP passphrase

This passphrase is used to implement encrypted Opportunistic Key Caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

Encrypt management frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don’t have the corresponding key.



As of WPA3, management frames have to be encrypted, so the value there is ignored and is assumed to be set as **Mandatory**. For WPA2, this is optional.

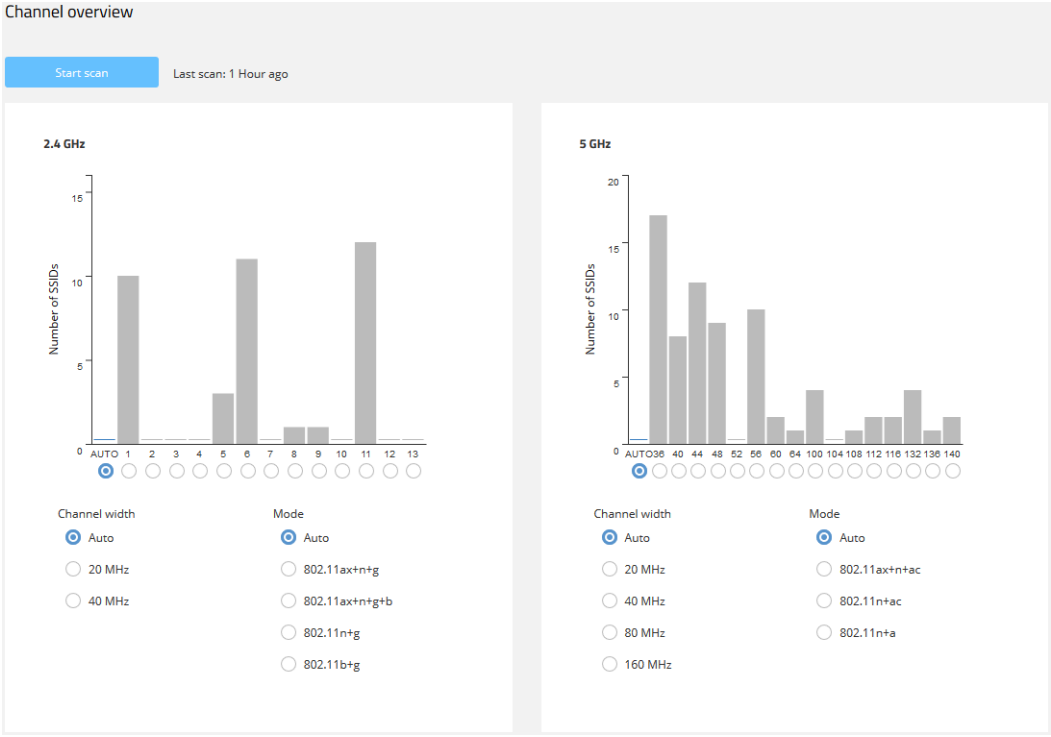
5.5.2.4 Technology

The **Technology** page offers the option to set fixed channels for the 2.4- and 5 GHz bands, to specify the available channel width and to determine which radio mode is used. The default setting for all options is automatic selection.



The physical settings that can be configured here apply to the entire frequency band and are not SSID-specific.

With automatic channel selection, the channel is not changed during operation. no change of the channel takes place during operation. The channel is only selected when the WLAN module is started.

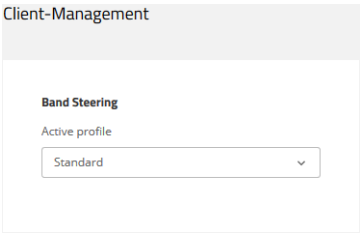


The two bar charts visualize how many SSIDs the device detected on the various 2.4- and 5 GHz channels, which can represent the potential load on the channels.

The bar charts only contain information if a neighborhood scan has been performed under **Neighborhood**.

Client Management

The settings for band steering for Wi-Fi networks can be found here. Band Steering allows clients to be routed from the overflowing 2.4 GHz frequency band to the 5 GHz frequency band, providing more bandwidth for each client and improving the user experience. LCOS LX provides the ability to route clients to the optimal frequency band for them using the 802.11v standard. Clients that do not support the 802.11v standard can also be routed to the 5 GHz band by delaying sample responses or by selectively disconnecting from the WLAN. See also *Band steering* on page 15.



Active profile

Select the profile that defines the settings for the band steering module.

Standard

Steering is based on the medium load and the detected interference on the current channel and is preferably done using 802.11v. If the client does not support 802.11v, steering is performed by means of a targeted disassociation of the client. Steering is performed both before association and, if necessary, while the client is already associated. This is the recommended profile.

Disabled

No steering is carried out at all. The client decides autonomously which frequency band to choose.

Legacy

Steering takes place before the client is associated by the targeted restraint of probe responses. The 5 GHz band is always preferred regardless of the workload.

5.5.2.5 QR code

This page provides access to a QR code for any open or WPA2-PSK secured SSID. The QR code can be scanned by current smartphones (an additional app may be required) and sets up the respective WLAN automatically on the smartphone. This spares users the laborious entry of a wireless key.

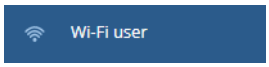
It is also possible to print out individual QR codes separately.



QR codes cannot be used for networks secured by 802.1X as they do not use a static WLAN key (PSK).

5.5.3 WLAN users

You reach this section in WEBconfig by means of the **Wi-Fi user** item in the sidebar.

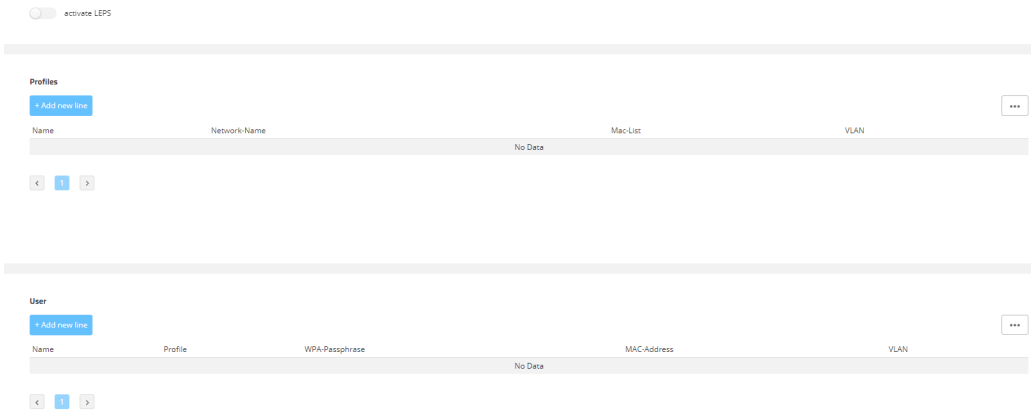


5.5.3.1 LEPS

When configured in LEPS, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. LEPS profiles are used to avoid having to repeat all of the settings for every new user. You then create the LEPS users with their individual passphrases and link them to one of the LEPS profiles created previously.

Alternatively, you can link the passphrase to a MAC address to set up a MAC address filter.

Here you configure the **Profiles** and **User** for the R&S®NC Enhanced Passphrase Security (LEPS). The switch **Activate LEPS** enables the LEPS feature.



5.5.3.1.1 Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users.

Name

Enter a unique name for the LEPS profile here.

Network-Name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

Mac-List

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

Only clients whose MAC address is not known are admitted.

VLAN

Here you specify which VLAN is assigned to a LEPS user or client who is connected to this profile.

5.5.3.1.2 Users

Create individual LEPS users here. Each LEPS user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.

Name

Enter a unique name for the LEPS user here.

Profile

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

Compared to simply assigning a passphrase to a user, managing a passphrase for each MAC address requires a bit more work, but you have greater control over the devices in the network.

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN configured here takes priority.

5.5.4 WDS (Wireless Distribution System) / Point-to-point links

You can reach this area in WEBconfig via the **WDS** item in the sidebar.



WDS can be used to set up point-to-point WLAN links between access points. These connections serve as a wireless backhaul, allowing remote access points to be connected to the rest of the

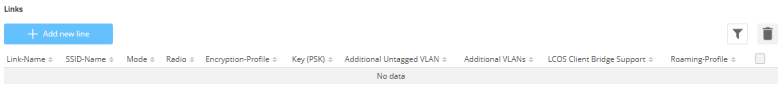
network. This allows WLAN coverage to be provided even in areas where access points cannot be connected via Ethernet, for example.

These access points optionally offer SSIDs for connecting WLAN clients (“repeater” mode) or for connecting the wireless backhaul to its Ethernet port (wireless bridge).

With LCOS LX 6.10, WDS operation is validated over a maximum distance of 300 meters.

5.5.4.1 Links

Configure here general settings relating to the WDS connection. Add a line to the table for each WDS connection. By default, the table is empty.



Link-Name

The name of the link. Used for further referencing in the device configuration.

SSID-Name

The name of the special SSID used for the WDS link. This name must match at both ends of the connection.

Mode

In the context of a WDS connection, there are three roles: Access Point, Client, Legacy Client. The partner configured as a client searches for a partner configured as an access point using the SSID configured above and initiates the connection. The access point configured as a legacy client can log into the SSID of any access point

In a point-to-multipoint scenario, multiple clients can connect to an access point.

The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above. In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

Encryption-Profile

The encryption profile to be used for the WDS link.

Key (PSK)

The WPA-PSK used for the WDS link. When using an encryption profile with 802.1X, this field can be left empty.

Additional VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

Additional Untagged VLAN

Untagged packets are to be transmitted.

LCOS Client Bridge Support

If the LCOS LX access point in client mode is connected to an LCOS access point in base station mode, 4-address frames can still be used for this, which enables the transmission of VLANs or MAC addresses. This mode cannot be used if the LCOS LX access point is operated in base station mode and an LCOS access point is logged in to it in client mode.

Roaming profile

Here you can enter a roaming profile if the access point is in client or legacy client mode.

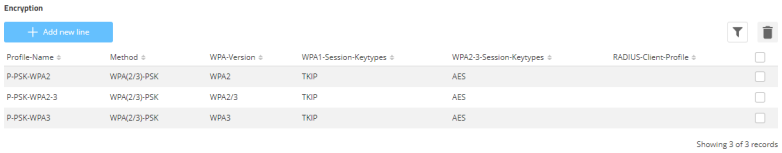
Optionally configure an encryption profile under *Encryption* on page 142.

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first under *RADIUS client profiles* on page 144.

If required, create a roaming profile under *Roaming profiles* on page 144.

5.5.4.2 Encryption

The settings for encryption and authentication of the Wireless Distribution System are configured here.



For WDS connections, we recommend using WPA3 to guarantee maximum security.

The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-PSK-WPA2

The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.

Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

Method

Here you configure the encryption method. The following methods are available:

WPA

WPA(2/3)-PSK: WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal.

RADIUS

WPA(2/3)-802.1X: WPA2 and/or WPA3 with RADIUS.

WPA-Version

Wi-Fi Protected Access (WPA) is an encryption method. Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA3: WPA version 3 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.
- WPA2/3: Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

WPA2/3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2 and 3. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

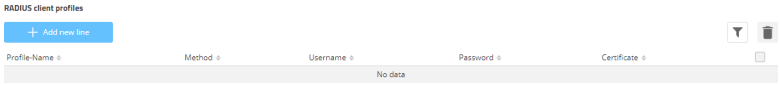
If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

RADIUS-Client-Profile

Specify a RADIUS client profile here if necessary.

5.5.4.3 RADIUS client profiles

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile here first.



Profile name

Use a unique profile name, which you specify later in the encryption profile.

Method

Select a method that suits your requirement. When using “TLS”, uploading a certificate is necessary.

Username

Enter the RADIUS user name here. When using the “TLS” method, no entry is necessary here.

Password

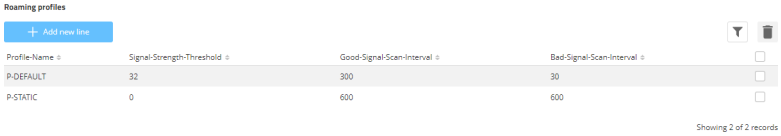
Enter the RADIUS password here. When using the “TLS” method, no entry is necessary here.

Certificate

You can accept the RADIUS server's certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server. See *Client certificate* on page 145 for the certificate upload.

5.5.4.4 Roaming profiles

If required, create a roaming profile here.



Profile name

Use a unique profile name, which you specify later in the WDS connection.

Signal-Strength-Threshold

Enter the threshold value from which the scan interval of the access point should change.

Good-Signal-Scan-Interval

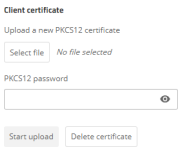
If the signal strength is above the limit, a scan is performed in seconds during this time to check if a better access point becomes available to connect.

Bad-Signal-Scan-Interval

If the signal strength falls to the specified limit, a scan is triggered directly to search for a better access point. If no better access point is available, the search continues in the specified time in seconds until a connection to an access point with a better signal strength could be connected or the signal with the connected access point has improved again.

5.5.4.5 Client certificate

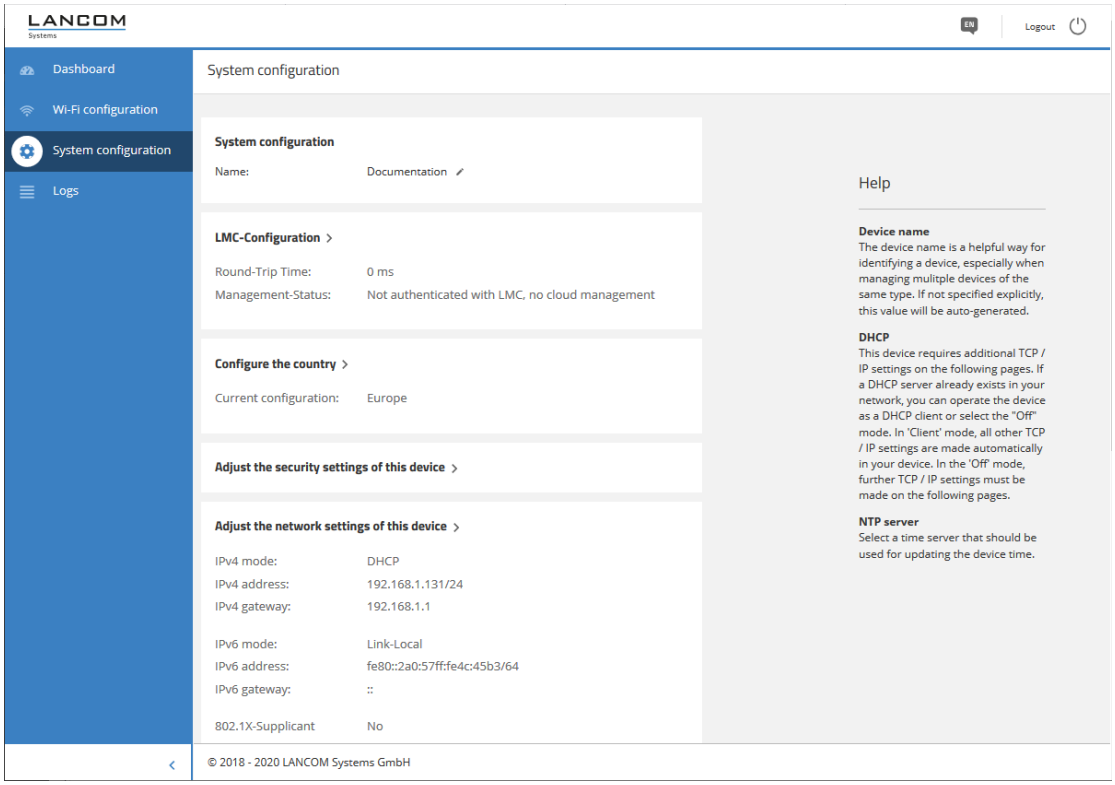
Manage the client certificates for the WDS connections here.



Select a PKCS12 container and specify the associated password. Use **Start upload** to upload the certificate to the device. You can delete any existing certificates via **Delete certificate**.

5.6 System configuration

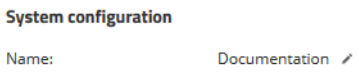
This allows you to configure the basic parameters of your device, such as the device name or the IP settings for managing the device.



You can edit individual fields such as the system name by clicking on the check mark next to it. An edit mask for the various sections opens after clicking on the headline.

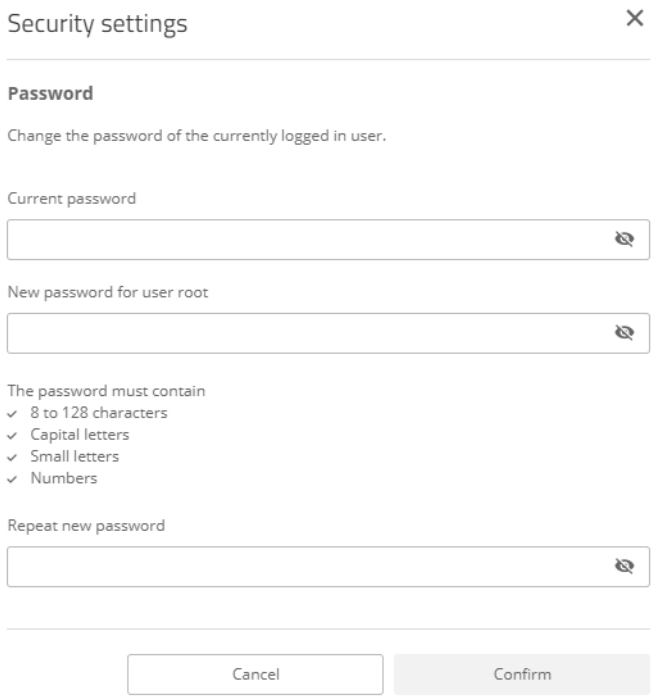
5.6.1 Name

Configure the device name here.



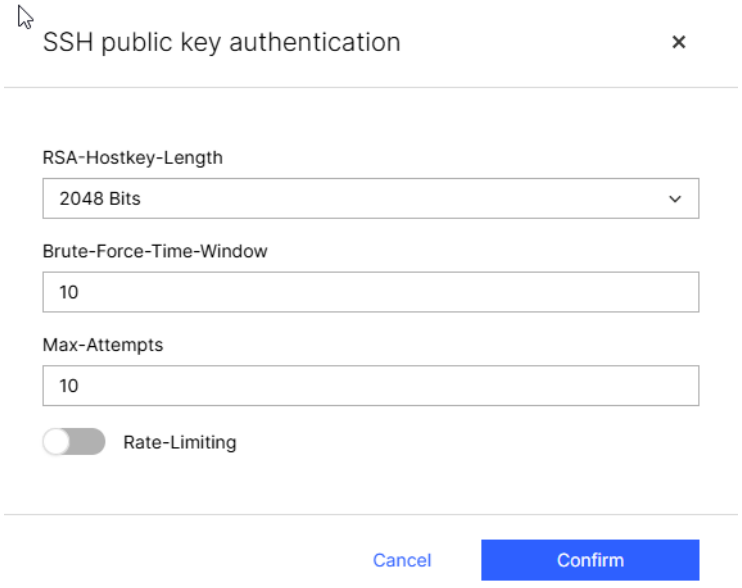
5.6.2 Security settings

Here you can change the password for the current user (usually “root”).



5.6.3 SSH Public Key Authentication

In WEBconfig, configure the settings for SSH public key authentication under **System configuration** > **Configure SSH public key authentication**.

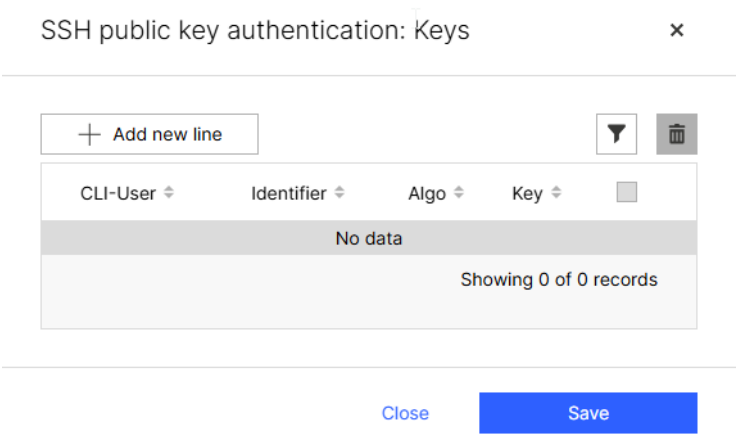


RSA-Hostkey-Length

You can select an SSH host key length between 2048 bits and 4096 bits. The host key is regenerated immediately after you change this setting.

Keys

In addition to interactive authentication using a user name and password, public key authentication can also be used.



CLI-User

The user for whom the public key entered below is to be valid. This can be either the “root” user or an optionally configured additional administrator (see *Additional Administrators* on page 23).

Identifier

The identifier is used to allow multiple public keys for the same CLI user, for example, if a separate public key was generated for each SSH client, but the login to LCOS LX should be performed using the same user account. In this case, enter the same CLI user but a different identifier.

Algo

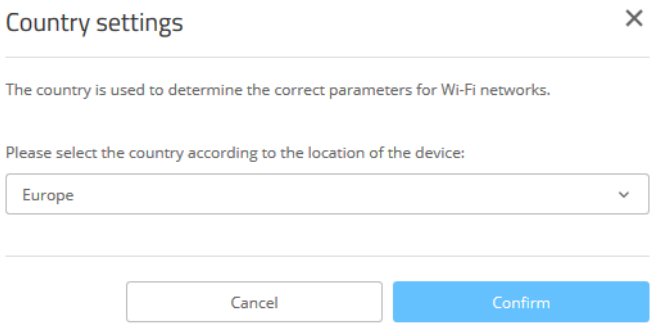
The algorithm used to generate the public key.

Key

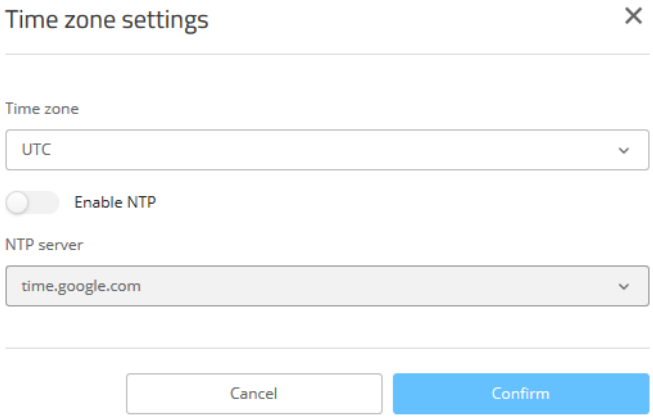
The public key to be used.

5.6.4 Country settings

Here you configure the country where the device is operated. Depending on this, the appropriate regulatory restrictions are set automatically.



5.6.5 Time zone settings



Time zone

Select a time zone. The default value is “UTC”.

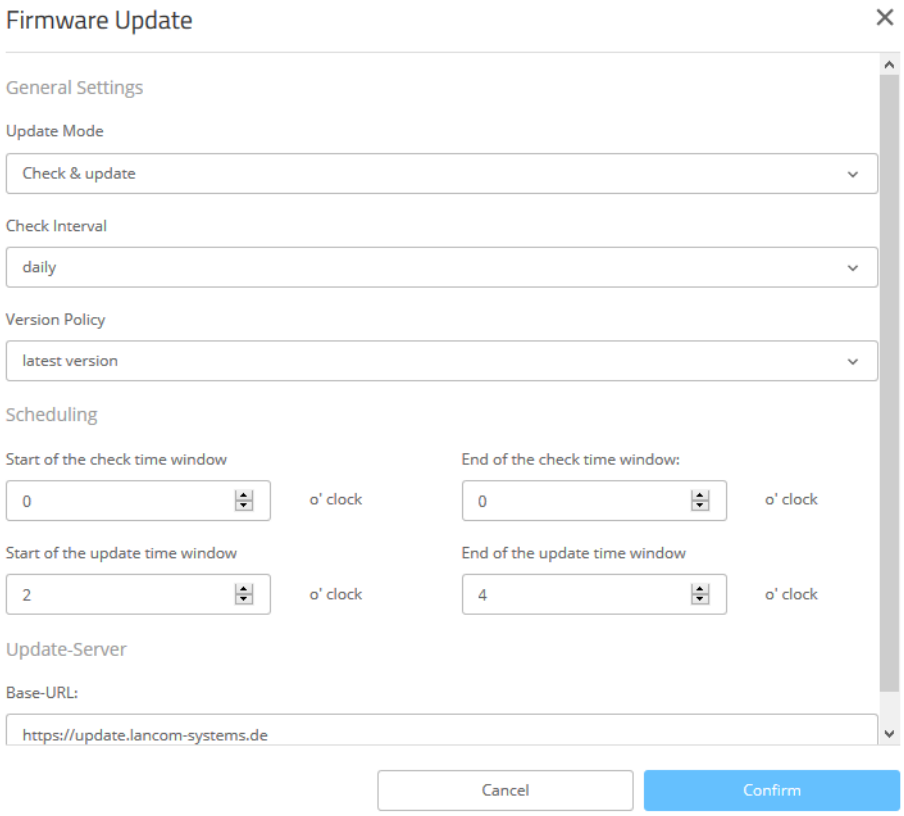
Enable NTP

Here you select whether the time should be obtained from a time server by means of the network time protocol (NTP).

NTP server

From this list you select a time server from which the time is to be obtained via NTP.

5.6.6 Automatic firmware update



Update mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but also to 5.00 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but not to 5.00 Rel.

Security patches only

The latest SU within a release. Example: 4.00 Rel is installed; an update to 4.00 SU1 is performed, but not to 4.00 RU2.

Latest version w/o REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 4.00 is installed; an update to 5.00 RU1 is performed, but not to 5.00 REL.

Check time window

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

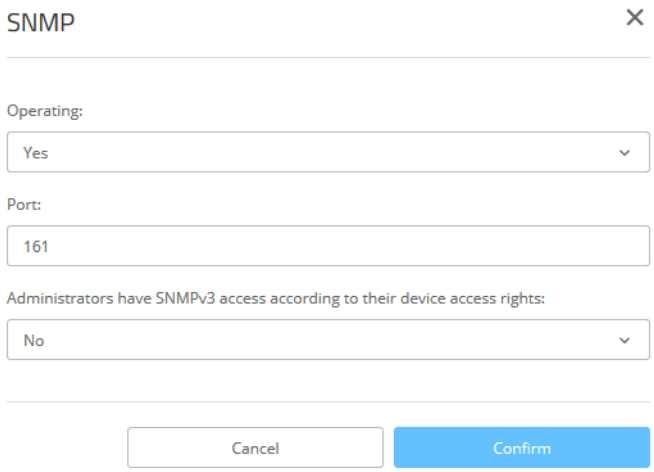
Update time window

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Base URL

Specifies the URL of the server that provides the latest firmware versions.

5.6.7 SNMP



Operation

Activate SNMP.

Port

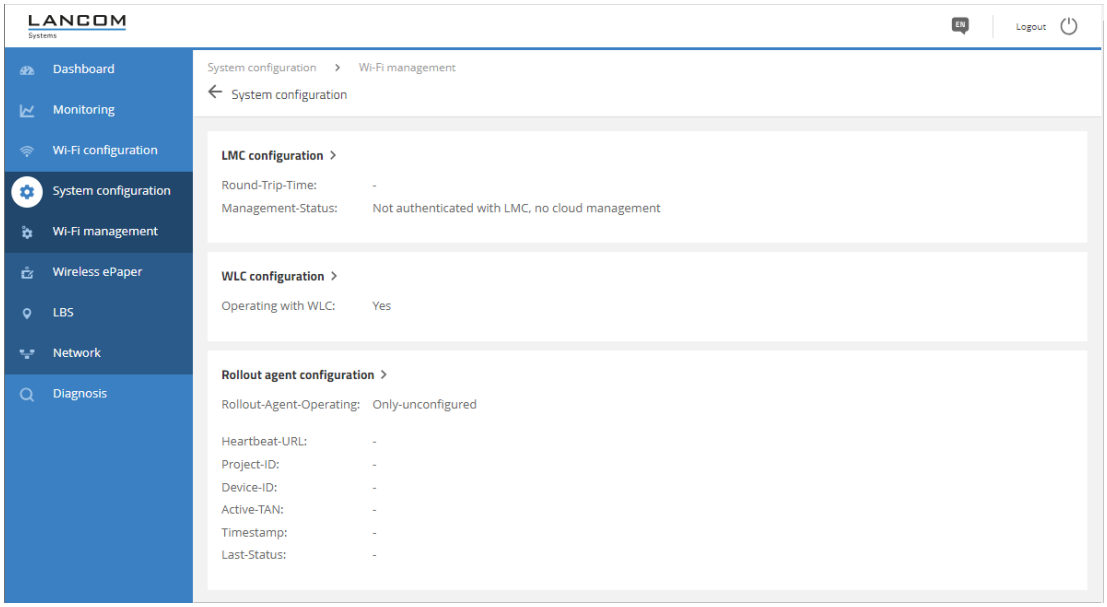
If necessary, adjust the port used for SNMP. Default: 161

Administrators have SNMPv3 access according to their access rights

Enable this option if registered administrators, including the root user, should also have access via SNMPv3.

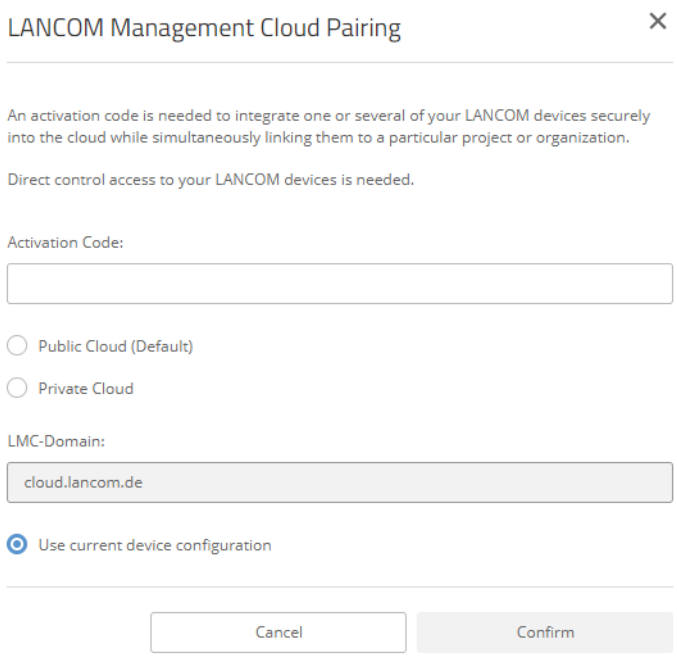
5.6.8 Wi-Fi management

In this section you will find settings for managing the access point via the R&S®LANCOM Management Cloud or a WLAN controller (WLC).



5.6.8.1 LMC configuration

Use the R&S®LANCOM Management Cloud to pair your device subsequently.



Activation code

Enter the activation code that you generated in your R&S®LANCOM Management Cloud project earlier.

Public Cloud

This option specifies the LMC domain of the Public Cloud from R&S®NC.

Private Cloud

With this option you can specify the LMC domain of your private instance of the R&S®LANCOM Management Cloud.

LMC domain

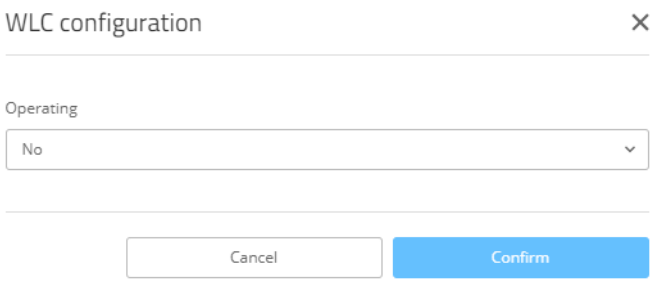
Shows either the LMC domain of the Public Cloud or you enter the LMC domain of your private instance of the R&S®LANCOM Management Cloud.

Use current device configuration

Applies the settings already configured in the device.

5.6.8.2 WLAN management

Specify here whether your device is managed by a WLAN controller.



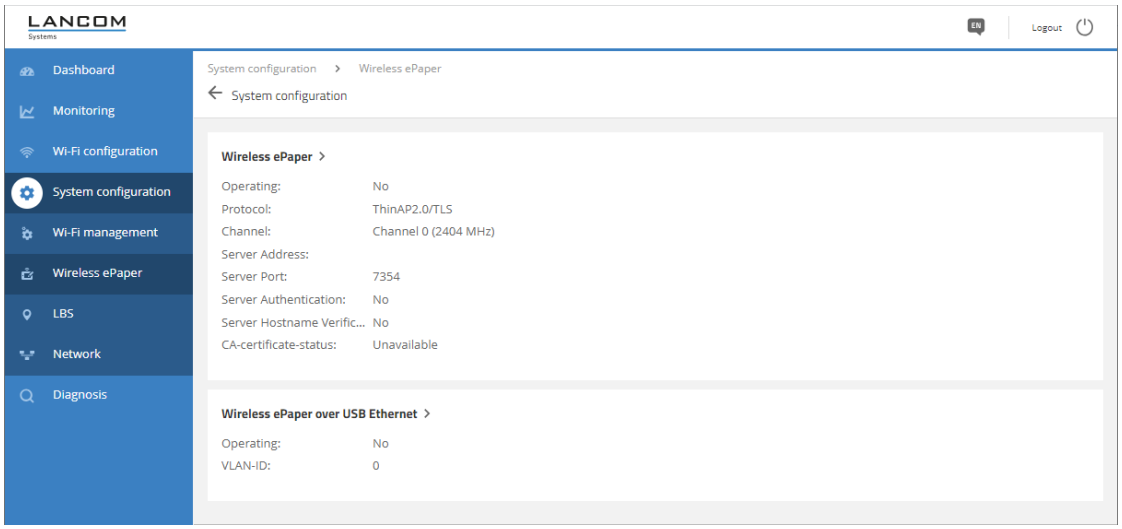
Operation

This configures whether an access point actively searches for a WLC and can be managed by one.

This option should be deactivated for operation in stand-alone mode.

5.6.9 Wireless ePaper

In this section you will find settings for Wireless ePaper.

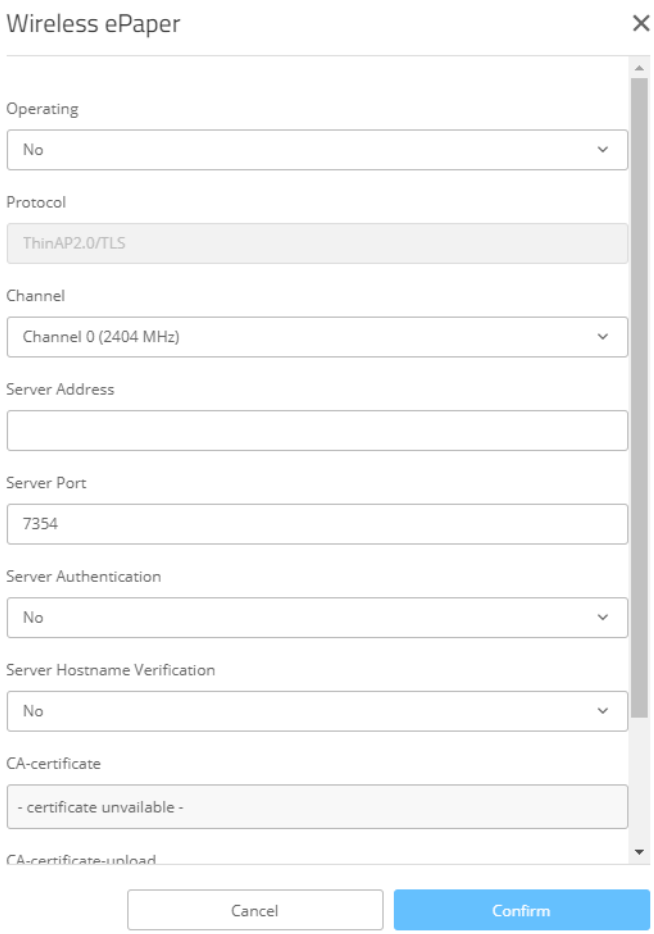


5.6.9.1 Wireless ePaper

R&S®NC Wireless ePaper Displays provide a variety of options for displaying information. You can automatically and remotely update the calendar schedule for your conference rooms, you can create dynamic notices and direction signs, or you can control the price labels of goods on your shelves from a central location in real time. The wide range of different settings allows you to set up your very own customized use case.

The settings for operating Wireless ePaper Displays are to be found in LANconfig under **Tools** > **Options** > **Wireless ePaper**. Under IP/hostname you enter the IP address and the port of the Wireless ePaper Server. The recommended port number is 8001.

You invoke the Wireless ePaper management in LANconfig under **Tools** > **Start Wireless ePaper management**.



Operating

Use this to activate the Wireless ePaper feature in the access point.

The server must be configured for the connection type ThinAP2.0/TCP. Please refer to the *R&S®NC Support Knowledge Base* for further information. Use the same method to set the following two configuration options to enable communication between the server and LCOS LX access points:

```
accessPointUseThinMode?value=true accessPointThinUseOutboundMode?value=true
```

This can be done, for example, with “curl” as follows:

```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true

curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

The legacy connection mode via UDP is not supported by LCOS LX.

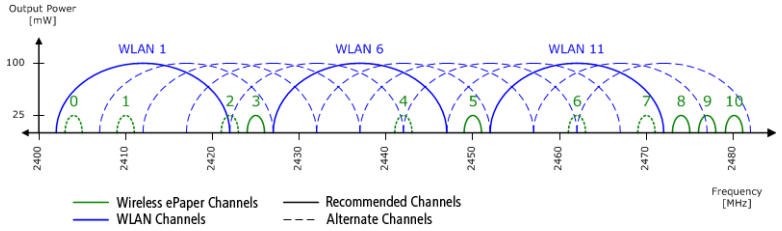
Protocol

The protocol used to communicate with the server.

Channel

Configure the radio channel to be used for controlling the Wireless ePaper Displays.

Depending on the radio channel used, connecting the server to a Display can take up to 30 minutes (channels 3, 5, 8, 9, 10) or up to 120 minutes (channels 0, 1, 2, 4, 6, 7). If possible, you should prefer the channels 3, 5, 8, 9 and 10, as Wireless ePaper Displays scan them more frequently and they do not interfere with the popular Wi-Fi channels 1, 6, and 11.



Do not select the same channel for two access points that are in the same area. This causes interference and prevents Displays from joining the network. It is possible to set the same channel on two access points if you are sure that each display is only within range of one of these access points.

Server address

Here you configure the IP address of the Wireless ePaper Server that the access point should contact.

Server port

The TCP destination port to be used for communication with the server.

Server Authentication

Optionally, the access point can check the server certificate of the Wireless ePaper Server when it connects to it. If this option is enabled, a corresponding CA certificate (or certificate chain) in PEM format must also be loaded onto the access point via WEBconfig.

Server Hostname Verification

In connection with the **Server Authentication** option, this setting decides whether the “Common Name” specified in the certificate is checked for a match with the host name of the addressed Wireless ePaper Server.

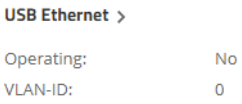
CA certificate

If you have uploaded a certificate to the device for server authentication, it will be displayed here.

CA-certificate-upload

If you use server authentication, a CA certificate for server verification must also be uploaded to the device. You can do this here by selecting the certificate file and then uploading it.

5.6.9.2 Wireless ePaper over USB Ethernet



Here you will find the settings for USB Ethernet support. Selected USB Ethernet devices are supported on access points with USB port. The CDC-EEM protocol is used here. For this purpose, the USB Ethernet device is hybridized with the LAN of the access point. It is possible to specify a VLAN ID for network segmentation. Therefore, make sure that the USB Ethernet device can communicate in your network and, if necessary, VLAN according to the manufacturer's specifications. The following USB Ethernet devices are qualified for operation with LCOS LX-based access points:

Operating

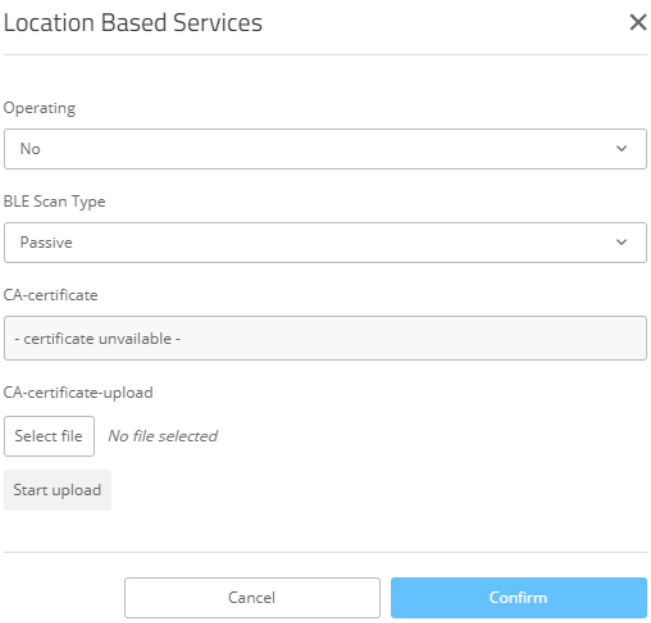
Switch on the USB Ethernet support here.

VLAN ID

Optional specification of a VLAN ID.

5.6.10 Location based services

R&S®NC access points are able to function as LBS clients with an LBS server. In this case, they report any connected clients to the LBS server, which can then offer location-based services to those clients. As of LCOS LX 5.30, an HTTP interface is supported. This must be configured via LANconfig, see *Location-based services (LBS)* on page 115.



Operation

By turning on the BLE radio here, data about the BLE environment is collected continuously.

BLE Scan Type

Choose between a passive and an active scan. The BLE name and a scan response can only be detected in the active scan. Note that BLE clients answering scan requests can increase power consumption.

CA certificate

If you have uploaded a certificate for the HTTPS protocol to the device, it will be displayed here.

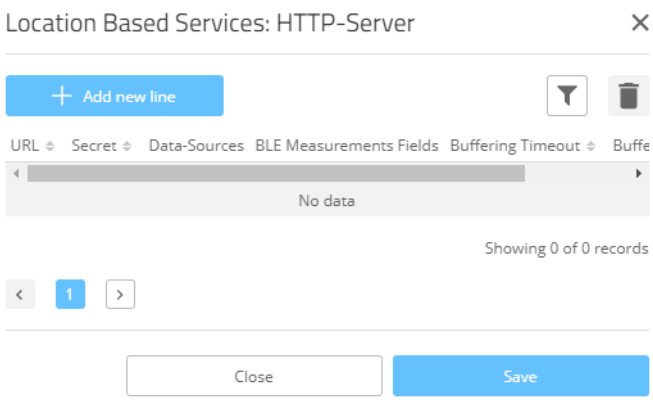
CA-certificate-upload

If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. You can do this here by selecting the certificate file and then uploading it.

The CA certificate must be uploaded in PEM format.

5.6.10.1 HTTP-Server

Under **HTTP-Server** you configure the HTTP endpoints for the LBS data.



URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. This can be done using WEBconfig. See *Location based services* on page 157.

Secret

The secret (key) is transmitted from the access point to the end point in the JSON messages and can additionally be used for message authentication.

Data-Sources

Here you configure the types of LBS data that should be sent. Only BLE is currently available.

BLE-Measurements-Fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.

Buffering Timeout

After the configured time (in seconds) is reached, all BLE messages buffered up to that point are sent to the server.

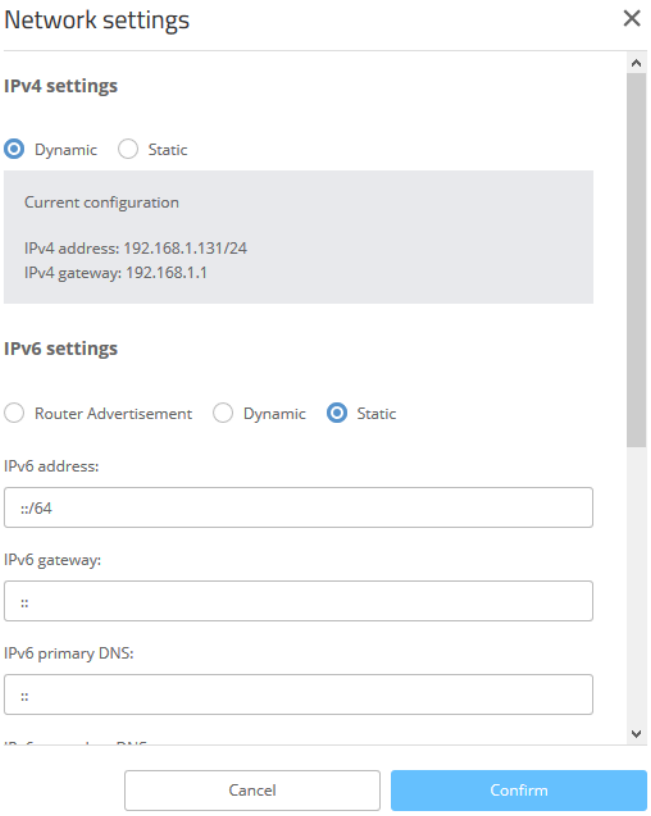
Buffer Size

After the configured data quantity (in bytes) is reached, all BLE messages buffered up to that point are sent to the server.

With the value for **Buffering Timeout** and **Buffer Size** both set to 0, the messages are sent to the server as soon as possible.

5.6.11 Network settings

Here you have the option to change network settings of your device, such as its IP address.



IPv4 settings

Dynamic

Uses DHCPv4 to configure the IPv4 parameters. This is the default value.

Static

Uses the IP parameters that you can configure in the fields **IPv4 address**, **IPv4 gateway**, **IPv4 primary DNS** and **IPv4 secondary DNS**.

Note that the IPv4 address must be specified in CIDR notation (for example, 192.168.1.1/24).

IPv6 settings

Router Advertisement

Uses router advertisements/SLAAC to configure the IPv6 parameters. If the received router advertisement contains the M (managed) flag, further parameters are obtained via DHCPv6.

Dynamic

Uses DHCPv6 to configure the IPv6 parameters.

Static

Uses the IP parameters that you can configure in the fields **IPv6 address**, **IPv6 gateway**, **IPv6 primary DNS** and **IPv6 secondary DNS**. This is the default value.

802.1X supplicant

These are the settings for the 802.1X supplicant functionality, which authenticates the device towards the LAN at a switch infrastructure secured by 802.1X.

User name

The user name to use to authenticate at the 802.1X infrastructure.

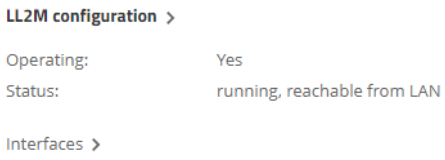
Password

The password to use to authenticate at the 802.1X infrastructure.

Method

The EAP method used to authenticate at the 802.1X infrastructure.

5.6.11.1 LL2M configuration



Operation

A basic pre-requisite for all methods device configuration is for an IP connection to exist between the configuration computer and the device. No matter whether you use LANconfig, WEBconfig or SSH; it is impossible to send any configuration commands to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. The only option in this case is to access the device via the serial configuration interface, which however is not available on all devices, or to reset the device to its factory settings. However, both options require physical access to the device—this may not always be the case for the concealed installation of access points and can represent considerable overhead for larger-scale installations.

The **R&S®NC Layer 2 Management Protocol (LL2M)** is used to also enable configuration access to a device even without an IP connection. All this protocol requires is a connection on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server, which then responds to the requests or runs the commands. Both the LL2M client and the LL2M server are integrated in the LCOS LX. The LL2M client commands are executed via the command line or WEBconfig.

An encrypted tunnel is set up for every LL2M command to protect the transmitted log-in information. To use the integrated LL2M client, start a terminal session on a device that has local access to the LL2M server via the available physical medium (LAN, WLAN). In this CLI session you can use the following commands to contact the LL2M server: `LL2Mdetect` and `LL2Mexec`. See *Command-line interface — command summary* on page 10

Enable LL2M here.

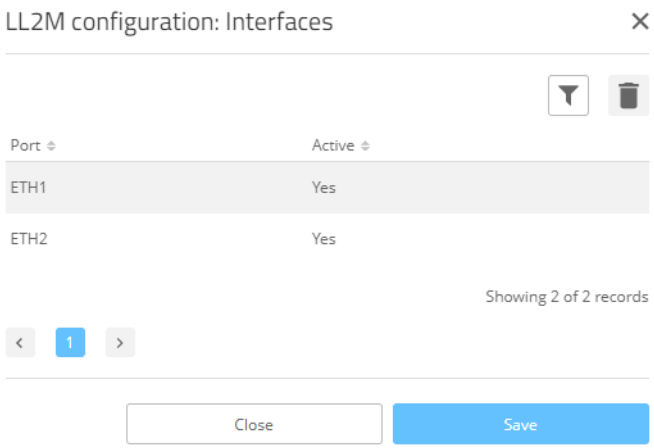
Access points of type LANCOM LW-500 can only be found and configured via LL2M if LL2M packets reach the access point with a VLAN tag which is included in the configuration of the access point (WLAN SSID configuration or management VLAN configuration).

Status

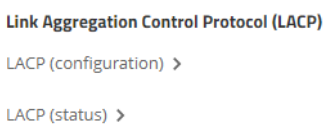
Shows the status of the current LL2M configuration.

Interfaces

This item is used to specify the interfaces or Ethernet ports where the LL2M server can be reached. The presetting provides accessibility on all Ethernet ports.



5.6.11.2 Link Aggregation Control Protocol (LACP)



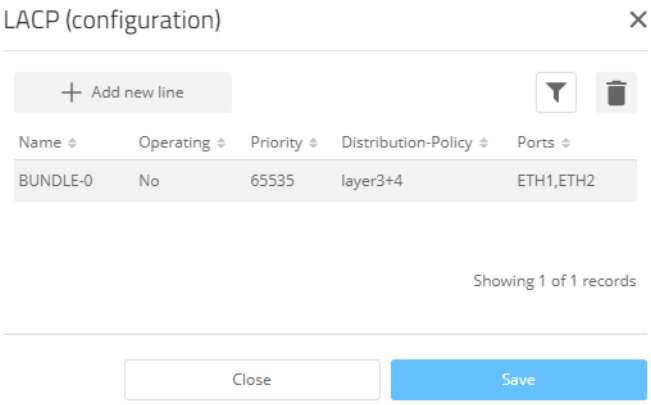
Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle LAN ports into a virtual link. Physical connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

LANconfig: **Interfaces** > **Port config** > **Link Aggregation**

5.6.11.2.1 L2TP Endpoints

The **LACP** menu is used to configure the Link Aggregation Control Protocol.



Name

This is the logical interface used to bundle the selected physical interfaces.

Operating

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together into one common logical bundled interface. In the disabled state the interfaces that are selected in the corresponding table still operate as individual interfaces.

Priority

Enter the LACP system priority. The default value is 65,535.

Distribution-Policy

There are a number of options for distributing the network packets to the various bundled interfaces. The following characteristics are used for distribution:

layer2

MAC addresses

layer2+3

A combination of MAC addresses and IP addresses

layer3+4

IP addresses and TCP/UDP ports

encap2+3

Like layer2+3. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

encap3+4

Like layer3+4. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

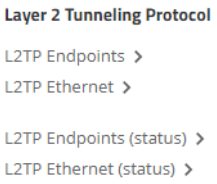
Ports

Use this parameter to select the physical interfaces as a comma-separated list that the device bundles via LACP. Default: ETH1,ETH2

5.6.11.2.2 LACP (Status)

The item **LACP (Status)** displays status information on the LACP connections.

5.6.11.3 Layer-3 Ethernet tunnel with L2TPv3



LCOS LX supports the Layer 2 Tunneling Protocol (L2TP) in version 3. With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers, and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

L2TP uses two types of data:

Control data

The control data are used to establish, maintain and tear down the tunnel connections. The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

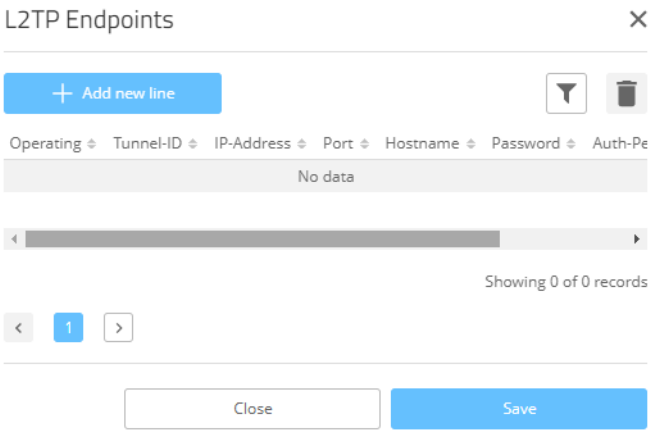
Payload data

The payload data are encapsulated in Ethernet frames, which are exchanged between the LAC and the LNS via the tunnel. In contrast to the control data, payload data contains no data flow control. Thus there is no guarantee that the sender and receiver are exchanging data correctly.

Unlike PPTP, which transfers control and payload data via different protocols (TCP and GRE), L2TP only uses UDP for both data types. You also have the option to operate multiple logical payload-data channels on each control-data channel.

5.6.11.3.1 L2TP Endpoints

Use **L2TP Endpoints** to configure the L2TP endpoints for the L2TPv3 tunnels. This configures the tunnel so that the control data makes an L2TP tunnel into a tunnel endpoint.



Tunnel ID

The name of the tunnel endpoint. For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Operating

This L2TP endpoint is enabled or disabled.

IP Address

The IP address of the tunnel endpoint.

Port

UDP port to be used. Default: 1701

Hostname

User name for the authentication For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Password

The password for the authentication This is also used to hide the tunnel negotiations, if the function is activated.

Auth-Peer

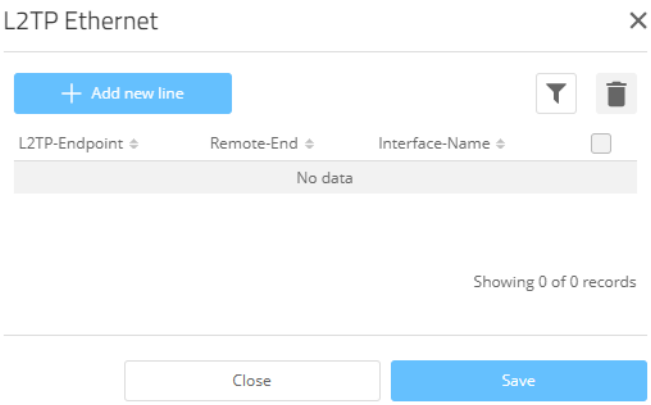
Specifies whether the remote station should be authenticated.

Hide

Specifies whether tunnel negotiations should be hidden by using the specified password.

5.6.11.3.2 L2TP Ethernet

The item **L2TP Ethernet** is used to configure the L2TPv3 tunnel between a WLAN network and an L2TP endpoint.



L2TP Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint.

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

Interface-Name

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

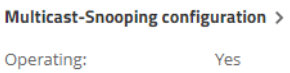
MTU

This setting adjusts the MTU of an L2TP Ethernet tunnel to the specified value, e.g. when connecting the tunnel across networks with smaller MTUs. Possible values: 68-1500

5.6.11.3.3 L2TP Status

Under **L2TP Endpoints (status)** and **L2TP Ethernet (status)**, you can see status information about the L2TP tunnels.

5.6.11.4 Multicast-Snooping configuration



All devices with WLAN interfaces have a “LAN bridge” that transfers data between the Ethernet ports and the WLAN interfaces. The LAN bridge works like a switch in many respects. The central task of a switch is to forward packets only to the port to which the receiver is connected. To do this, the switch automatically forms a table from the incoming data packets in which the sender MAC addresses are assigned to the ports.

If a destination address of an incoming packet is found in this table, the switch can forward the packet specifically to the correct port. If the destination address is not found, the switch forwards the packet to all ports. This means that a switch can only forward a packet specifically if the

destination address has already been received by it once as the sender address of a packet via a specific port. However, broadcast or multicast packets can never be entered as the sender address in a packet, which is why these packets are always “flooded” to all ports.

While this behavior is the correct action for broadcasts, since broadcasts should eventually reach all possible recipients, it is not necessarily the desired solution for multicasts. Multicasts are usually aimed at a specific group of recipients on a network, not all of them.

For example, video streams are often multicast, but not all stations on the network should receive a particular stream.

Various applications in the medical field use multicasts to transmit data to specific terminals that should not be viewed at all stations.

With a LAN bridge in the device, there will therefore also be ports to which no single receiver of the multicast is connected. The “unnecessary” sending of multicasts on ports without receivers is not a mistake, but it leads to performance problems, especially in WLAN networks. There, the unnecessary sending of multicasts can lead to a significant restriction of the available bandwidth, since multicasts in the WLAN—just like broadcasts—are sent at the lowest possible transmission rate so that they can be received by every WLAN subscriber.

With the Internet Group Management Protocol (IGMP) for IPv4 as well as Multicast Listener Discovery (MLD) for IPv6, the TCP/IP protocol family provides a protocol with which the network stations can inform the router to which they are connected of their interest in certain multicasts. To do this, the stations register with the routers for specific multicast groups from which you want to obtain the corresponding packets (multicast registration). IGMP uses special messages to register (join messages) and deregister (leave messages) for this purpose.

Multicast snooping makes use of these messages to decide to which port (i.e., also to which WLAN SSID) multicasts must be sent.

Operating

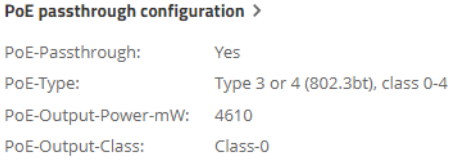
Turn multicast snooping on or off.

In addition, optional conversion of multicast data streams to unicast is possible. After activation of the feature, multicast data streams that are transmitted via WLAN interfaces are converted into individual unicast data streams for each client on the MAC layer or WLAN layer. The packets are duplicated for each client, but since they are now unicasts, they can be transmitted at the highest possible data rate for this client. Even though the packets are now duplicated, in most scenarios, the much faster transmission consumes much less airtime, which is then available for other transmissions. See *Multicast-to-Unicast* on page 62.

5.6.11.5 PoE Passthrough configuration

For models with the PoE Passthrough feature, supplying the access point with PoE 802.3bt (60W) allows a further PoE device (PD) to be connected to the second Ethernet port ETH2, and this in turn can be fed with a maximum of 30W.

This item switches the PoE Passthrough feature on and off. In the factory default settings it is deactivated. Further status information is displayed here or via the LANmonitor.



PoE Passthrough

The PoE Passthrough feature is switched on or off here.

PoE Type

Information about the PoE type.

PoE output-Power-mW

Status information about the energy output in milliwatts.

PoE Output-Class

Status information about the PoE output class.

6 Diagnosis

6.1 Trace output

Trace output can be used to check the internal processes in the device during or after configuration. Experienced users can read this output and discover any errors in connection establishment. One particular advantage is: The error may be located in the configuration of your own device or in the peer device.

Trace output has a slight time delay from the actual event, but the order of events is always recorded correctly. This generally does not influence the interpretation of the display, but this should be considered when making precise analyses.

6.1.1 Trace – an overview

Trace output is started in a CLI session. Set up an SSH session to the device. Call the trace with the following syntax:

```
> trace [--log] [+|-|#|?] <Parameter>
```

The command trace, the key and the parameters are each separated by a space. The keys control the trace while the parameter determines the actual output.

Table 2: Overview of keys

Key	Meaning
`--log`	Output of “historical” Information from the log
`?`	displays help
`+`	switches trace output on
`-`	switches trace output off
`#`	Toggles “”between the different trace outputs
no key	displays the current status of trace

Table 3: Overview of parameters

Parameter	Meaning	`--log`
WLAN	WLAN-related outputs, such as client log ins and log offs, key negotiation, ... If the trace is not enabled, the log file will contain only a small amount of information and the “historical” output will not be particularly informative.	Yes
IAPP	Output on IAPP (inter access point protocol)	Yes
Kernel	Output on the basic system and kernel.	Yes
SSH	Output on the SSH service.	Yes

Parameter	Meaning	`--log`
*	Wildcard, which stands for all services.	Depends on the service

6.1.2 Trace – operation

The following examples illustrate the functions of trace:

- Start one or more traces:

```
trace + ssh kernel
```

- Stop traces:

```
trace - ssh kernel
```

- Stop all traces:

```
trace - *
```

- Toggle between “”switching the traces on and off:

```
trace # ssh kernel
```

- Output “historical” information, if supported and available in the log:

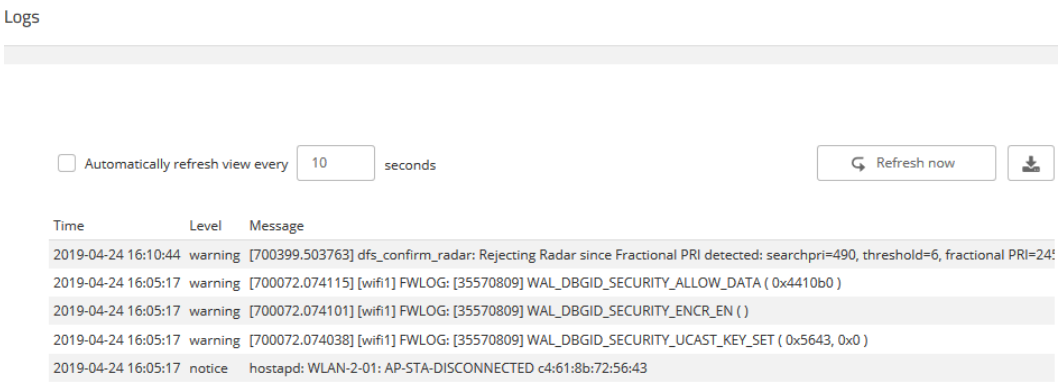
```
trace --log + kernel
```

6.2 Logs in WEBconfig

You reach the “Logs” area by means of the **Diagnosis** > **Logs** item in the sidebar.



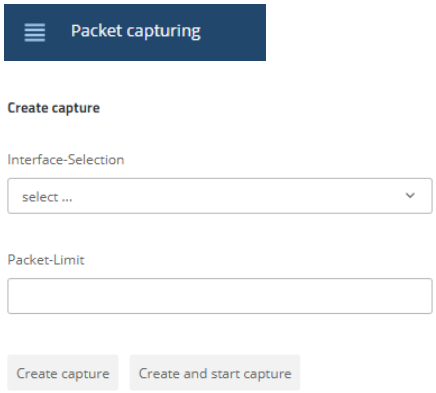
This area outputs the device SYSLOG.



6.3 Packet capturing in WEBconfig

This item allows you to capture Wireshark-compatible packets.

You reach this section from the sidebar under **Diagnosis** > **Packet capturing**.

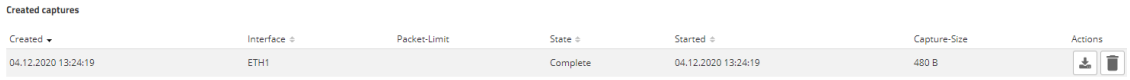


In the section “Created captures” you can specify the interface where packets are to be captured and whether the capture size should be limited by the number of captured packets.

The interfaces available for selection include all Ethernet interfaces as well as active WLAN SSIDs (separated according to frequency band).

Click on **Create capture** and a capture job is created with the chosen settings, but it is not yet started. The capture can then be started at any time from the “Created captures” list. Click on **Create and start capture** to create a capture job with the chosen settings and start it immediately.

Using the “Created captures” list you can start, stop and download captures as a .pcap file.



Capture data is streamed directly from the access point or WEBconfig into the browser's cache. Please note that a capture job that has been started is aborted when you close WEBconfig.

Different capture jobs can be started in parallel.

6.4 Monitoring of Access Point Position and Mounting Angle

This feature is used to monitor the mounting angle of an access point equipped with the appropriate sensor. Models like the R&S®NC LX-7500 and the R&S®NC LX-7300 are primarily optimized for ceiling mounting, although wall mounting is also possible. This sensor allows compliance with proper mounting to be verified without an on-site inspection.

The access point reports the general mounting orientation Ceiling / Wall / Floor. “Floor” refers to a mounting with antennas / top side facing upwards. Additionally, the angle or tilt of the access point is reported.

The reported values can be read via the CLI under **Status** > **Hardware Info** > **Mounting Type** (1.47.11) or **Status** > **Hardware Info** > **Mounting Angle** (1.47.12). **Mounting Type** can return the values Unknown, Ceiling, Wall, and Floor. **Mounting Angle** contains a degree value.

The status information is displayed in LANmonitor under the system information of the access point.

6.5 PoE Status Information

Access points with the appropriate module enable detailed monitoring of the PoE power supply.

To do this, the access point reports the respective status via the CLI under **Status** > **Hardware Info** > **Power**, using several values. These can also be displayed in LANmonitor under the system information and interfaces of the access point.

PoE-Type (1.47.42.1)

Displays the connected PoE power source in a single line, rather than per port as in the “Ports” table. If two PoE power sources are connected, a string like “802.3bt-Type-3 + 802.3bt-Type-3” is displayed.

Ports (1.47.42.6)

The following information is displayed for each port of the access point:

PoE-in-Type

Indicates the type of power supply: 802.3af-Type-1-or-802.3at-Type-2, 802.3bt-Type-3, 802.3af-Type-1, 802.3at-Type-2, or no-PoE.



The IEEE 802.3af Type 1 and IEEE 802.3at Type 2 types cannot be clearly distinguished and are therefore displayed as a single value.

PoE-in-Class

The class precisely specifies how much power (in watts) is available to the device. The following classes are possible: Class-0, Class-1, Class-2, Class-3, Class-4, Class-5, Class-6, Class-7, and Class-8. The class “None” is displayed when no PoE signal is present.

LLDP-Power-Negotiation

In addition to class-based negotiation, LLDP negotiation is also available at a higher level. This allows the PD (the access point) and the PSE (Power Source Equipment, the switch) to negotiate power in watts more granularly. This is optional and is not performed by all switches. If used, the expected behavior is that the switch initially activates only PoE in IEEE 802.3af Class-0 or similar (i.e., very low power), and higher power is activated only through LLDP negotiation with the access point. In this case, type and class will remain at a low level, but the actual negotiated power can be seen in “PoE-Power-Allocated-W”.



Please note that “PoE-Power-Allocated-W” always shows the maximum of class-based and LLDP-based negotiation. Therefore, if LLDP is absent but Class-6 was negotiated, 51W will be shown.

Device-Functions (1.47.42.7)

WLAN-Streams-2.4GHz

Indicates the possible WLAN streams in the 2.4 GHz band: Off, One, Two, Three, or Four.

WLAN-Streams-5GHz

Indicates the possible WLAN streams in the 5 GHz band: Off, One, Two, Three, or Four.

WLAN-Streams-6GHz

Indicates the possible WLAN streams in the 6 GHz band: Off, One, Two, Three, or Four.

WLAN-Scan-Radio

Indicates whether the scan radio is active.

USB-Port

Indicates whether the USB port is active.

Failover-Status (1.47.42.10)

The following statuses are possible:

Ready

If both PoE sources are active according to IEEE 802.3bt, it waits for a failover condition to occur, such as power loss on one of the two cables.

Engaged

A failover condition has been met, and the access point is now in failover status.

Disabled

Failover function has been disabled in settings, as “Load-Sharing” is configured instead of “Failover”.

Power-Status (1.47.42.11)

Indicates whether the access point has enough power to enable all functions, such as all WiFi radios, USB, etc. (“Fully operational”). If insufficient power is available, the value “Reduced function set” is displayed. You can check the “Device-Functions” table to see which functions are specifically disabled.

Dual-PoE-Mode (1.47.42.12)

The configured mode.

Hitless Failover

Allows uninterrupted operation of the access point if the PoE supply fails on one of the two Ethernet ports. The access point will not restart. This mode requires that the same PoE power is provided on both Ethernet ports.

In the case of the LX-7500, IEEE 802.3bt (Class 6 / 51W) is required for full operation.

Load Balancing

The access point draws power simultaneously via PoE from both Ethernet ports. Usually, the power drawn from both ports is similar, but ultimately this is influenced by the applied voltage and is therefore dependent on the specific circumstances.

This enables full operation of the R&S®NC LX-7500 with 2x IEEE 802.3at (Class 4 / 25.5W).

7 Factory default active services according to EN 18031 GEC-4

In LCOS LX , the following network services are active in the factory default state:

Service	Function	Port
SSH	Device management	TCP 22
HTTPS	Device management	TCP 443
LL2M	Device management	Layer 2
WTP	WLAN controller connection	UDP 1027
LMC	Connection to LANCOM Management Cloud	TCP 443
TFTP	Device search with LANconfig	UDP 69