LCOS LX 7.20

Menu Reference

10/2026

ROHDE&SCHWARZ
Make ideas real

Contents

1 Introduction....7
1.1 Components of the documentation....7
1.2 LCOS LX, an operating system from R&S®NC....7
1.3 Validity....8
1.4 Command-line interface — access....8
1.5 Command-line interface — menu structure....8
1.6 Command-line interface — command summary....9
2 Setup....14
2.1 Name....14
2.9 SNMP....14
2.9.1 Send-Traps....14
2.9.21 Port....15
2.9.27 Communities....15
2.9.28 Groups....16
2.9.29 Accesses....18
2.9.30 Views....21
2.9.32 Users....22
2.9.34 Target-Addresses....26
2.9.35 Target-Params....27
2.9.37 Admitted-Protocols....29
2.9.38 Allow-Admins....30
2.9.41 Operating....30
2.11 Config....31
2.11.1 Comment-1....31
2.11.2 Comment-2....31
2.11.3 Comment-3....31
2.11.4 Comment-4....32
2.11.5 Comment-5....32
2.11.6 Comment-6....32
2.11.7 Comment-7....32
2.11.8 Comment-8....33
2.11.9 Location....33
2.11.10 Administrator....33
2.11.11 Config-Aging-Minutes....34
2.11.18 LED-Mode....34
2.11.20 Cron-Table....34
2.11.21 Admins....37
2.11.50 LL2M....38
2.11.51 Tacacs-Plus....40
2.11.52 SSH....43

2.11.90 LED-Off-Seconds....45
2.11.91 LED-Test....45
2.11.99 Root-Hashed....45
2.11.130 PoE-Passthrough....46
2.14 Time....46
2.14.15 Holidays....46
2.14.16 Timeframes....47
2.14.20 Timezone....48
2.14.21 NTP....49
2.20 WLAN....50
2.20.1 Network....51
2.20.2 Country....62
2.20.3 Encryption....63
2.20.4 Band-Steering....71
2.20.5 Client-Isolation-Allowed....78
2.20.8 Radio-Settings....79
2.20.9 Automatic-Environment-Scan-Enabled....87
2.20.10 Automatic-Environment-Scan-Time-Begin....87
2.20.11 Automatic-Environment-Scan-Time-End....87
2.20.12 Hotspot....87
2.20.13 WDS....91
2.20.14 Include-UUID....98
2.20.15 Power-Saving-Mode....99
2.20.16 Include-Devicename....99
2.20.18 Client-Management....100
2.20.19 Client-Management-Mode....102
2.20.20 End2End-Test....103
2.20.133 LEPS....117
2.20.1111 Rate-Selection....120
2.22 Syslog....123
2.22.2 Server....123
2.23 Logging....124
2.23.1 Operating....125
2.23.2 Timer-Seconds....125
2.23.3 Level....125
2.23.4 Target....126
2.23.5 Trace....126
2.23.6 Log-Persistence....127
2.30 RADIUS....127
2.30.3 RADIUS server....127
2.30.4 Delete-WLAN-Supplicant-Certificates....130
2.30.11 LAN-Supplicant....130
2.30.12 WLAN-Supplicant....132
2.40 Multicast-Snooping....133

2.40.1 Operating....134
2.45 Bridge....134
2.45.1 DHCP-Snooping....134
2.46 mDNS-Filter....136
2.46.1 Services....136
2.46.2 Services-List....137
2.47 Firewall....137
2.47.1 Rules....138
2.47.2 Host-Groups....140
2.47.3 Log-Actions....141
2.59 WLAN-Management....142
2.59.1 Static-WLC-Configuration....142
2.59.2 Operating....143
2.59.3 Update-Cert-Before....143
2.59.4 Capwap-Port....143
2.60 Power....144
2.60 Dual-PoE-Mode....144
2.61 L2TP....145
2.61.1 Endpoints....145
2.61.2 Ethernet....148
2.62 LAN....149
2.62.1 LACP....149
2.62.2 Ethernet ports....152
2.62.3 Spanning-Tree....153
2.70 IP-Configuration....157
2.70.4 Static-Parameters....158
2.70.6 LAN-Interfaces....159
2.70.8 Untagged-VLAN....162
2.99 LBS....163
2.99.1 HTTP-Server....163
2.99.2 Operating....165
2.99.3 LBS-Server-Type....165
2.99.4 BLE-Scan-Type....166
2.99.5 Run-Bluetooth-Scan....166
2.99.6 Delete-CA-Certificate....166
2.99.7 Delete-Scan-Results....166
2.102 LMC....167
2.102.1 Operating....167
2.102.2 Proxy....167
2.102.7 Delete-Certificate....169
2.102.8 DHCP-Client-Auto-Renew....169
2.102.13 Configuration-Via-DHCP....169
2.102.15 LMC-Domain....170
2.102.16 Rollout-Project-ID....170

2.102.17 Rollout-Location-ID....170
2.102.18 Rollout-Device-Role....171
2.102.200 Pairing-Token....171
2.107 Automatic-Firmware-Update....171
2.107.1 Mode....171
2.107.2 Check-Firmware-Now....172
2.107.3 Update-Firmware-Now....172
2.107.4 Cancel-Current-Action....172
2.107.5 Reset-Updater-Config....173
2.107.6 Base-URL....173
2.107.7 Check-Interval....173
2.107.8 Version-Policy....173
2.107.10 Check-Time-Begin....174
2.107.11 Check-Time-End....174
2.107.12 Install-Time-Begin....175
2.107.13 Install-Time-End....175
2.111 IoT....175
2.111.1 USB....176
2.111.88 Wireless ePaper....176
3 Firmware....185
3.2 Table-Firmsafe....185
3.2.1 Position....185
3.2.2 Status....185
3.8 Switch firmware....186
3.10 Boot-count....186
4 Other....187
4.1 Reset-Config....187
4.2 Reboot....187
4.3 Delayed-Reboot....187
4.3 Cancel-Delayed-Reboot....188
4.5 Delete-Support-Info....188
1 Status....189
1.62 Syslog....189
1.62.1 Last-Messages....189

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

The 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 Guide comprehensively 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 *www.lancom-systems.com/downloads*.

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.

1.4 Command-line interface — access

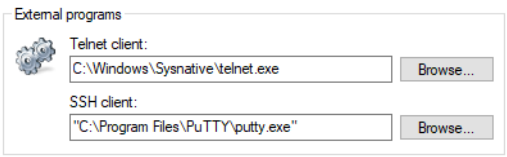
Access to the LCOS LX command-line interface (CLI) is via SSH. Use an SSH client such as PuTTY to connect to the IP address of the device.

Access credentials for a device in its delivery state are:

Username: root

Password: <Empty> (no password is set)

In LANconfig you configure your preferred SSH client under **Tools** > **Options** > **Extras** > **SSH client**:



To open an SSH session, use the context menu of the device and go to **WEBconfig / Console session** > **Open SSH session**.

1.5 Command-line interface — menu structure

The LCOS LX command-line interface is structured as follows:

Status

Contains the status and statistics of all internal modules in the device. These are not described here as we recommend that you use the GUI available in WEBconfig. Alternatively, you can download the Management Information Base (MIB) for your device, which contains the entries and a short description for use with SNMPv3. You can download the device MIB from *Download-Bereich*.

Setup

Contains all adjustable parameters of all internal modules in the device. See *Setup*.

Other

Contains actions such as resetting or rebooting. See *Other*.

1.6 Command-line interface — command summary

The command-line interface is operated with the following commands.

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.
`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.

2 Setup

This menu allows you to adjust the settings for this device.

Console path:

/

2.1 Name

Configure the device name here. For display purposes only.

Console path:

Setup

Possible values:

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

Default:

empty

2.9 SNMP

This menu contains the configuration of SNMP.

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

Console path:

Setup

2.9.1 Send-Traps

When serious errors occur, for example when an unauthorized attempt is made to access the device, it can send an error message to one or more SNMP managers automatically. Activate the option and, in the Target addresses table, add the targets where these SNMP managers are installed.

Console path:

Setup > **SNMP**

Possible values:

Yes
No

Default:

No

2.9.21 Port

Using this parameter, you specify the port which external programs such as LANmonitor use to access the SNMP service.

Console path:

Setup > **SNMP**

Possible values:

0 … 65535

Default:

161

2.9.27 Communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect 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.

This table is used to configure the SNMP communities.

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

Console path:

Setup > **SNMP**

2.9.27.1 Name

Enter a descriptive name for this SNMP community.

Console path:

Setup > **SNMP** > **Communities**

Possible values:

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

Default:

empty

2.9.27.3 Security-Name

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

Console path:

Setup > **SNMP** > **Communities**

Possible values:

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

Default:

empty

2.9.27.8 Status

This entry is used to enable or disable this SNMP community.

Console path:

Setup > **SNMP** > **Communities**

Possible values:

Active
The community is enabled.

inactive
The community is disabled.

Default:

Active

2.9.28 Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users.

Console path:

Setup > **SNMP**

2.9.28.1 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.

You select a security model here as is appropriate.

Console path:

Setup > **SNMP** > **Groups**

Possible values:

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. Users can authenticate and communicate according to the following security levels:

NoAuthNoPriv

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

AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

Default:

SNMPv3_USM

2.9.28.2 Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Console path:

Setup > **SNMP** > **Groups**

Possible values:

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

Default:

empty

2.9.28.3 Group-Name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

Console path:

Setup > **SNMP** > **Groups**

Possible values:

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

Default:

empty

2.9.28.5 Status

Activates or deactivates this group configuration.

Console path:

Setup > **SNMP** > **Groups**

Possible values:

Active
inactive

Default:

Active

2.9.29 Accesses

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

Console path:

Setup > **SNMP**

2.9.29.1 Group-Name

Here you select the name of a group that is to receive these assess rights.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

2.9.29.3 Security-Model

Activate the appropriate security model here.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

Any
Any model is accepted.

SNMPv1
SNMPv1 is used.

SNMPv2_C
SNMPv2c is used.

SNMPv3_USM
SNMPv3 is used.

Default:

Any

2.9.29.5 Read-View-Name

Set the view of the MIB entries for which this group is to receive read rights.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

2.9.29.6 Write-View-Name

Set the view of the MIB entries for which this group is to receive write rights.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

2.9.29.7 Notify-View-Name

Set the view of the MIB entries for which this group is to receive notify rights.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

2.9.29.8 Status

Activates or deactivates this entry.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

Active
inactive

Default:

Active

2.9.29.10 Min-Security-Level

Specify the minimum security level for access and data transfer.

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

NoAuthNoPriv

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.

AuthNoPriv

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

AuthPriv

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.

Default:

AuthPriv

2.9.30 Views

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

Console path:

Setup > **SNMP**

2.9.30.1 View-Name

Give the view a descriptive name here.

Console path:

Setup > **SNMP** > **Views**

Possible values:

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

Default:

empty

2.9.30.3 OID-Subtree

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

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

Console path:

Setup > **SNMP** > **Views**

Possible values:

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

Default:

empty

2.9.30.4 Type

Here you decide whether the OID subtrees specified in the following are “Included” or “Excluded” from the view.

Console path:

Setup > **SNMP** > **Views**

Possible values:

Included

This setting outputs MIB values.

Excluded

This setting blocks the output of MIB values.

Default:

Included

2.9.30.6 Status

Activates or deactivates this view.

Console path:

Setup > **SNMP** > **Views**

Possible values:

Active
inactive

Default:

Active

2.9.32 Users

This menu contains the user configuration.

Console path:

Setup > **SNMP**

2.9.32.2 Username

Specify the SNMPv3 user name here.

Console path:

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

Possible values:

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

Default:

empty

2.9.32.5 Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

Console path:

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

Possible values:

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-96 (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).

2.9.32.6 Authentication-Password

Enter the user password necessary for authentication here.

Cleartext input is only possible if the parameter in *2.9.32.14 Authentication-Password-Type* on page 25 was changed.

Console path:

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

Possible values:

Max. 130 characters from `anything printable`

Default:

empty

2.9.32.8 Privacy-Protocol

Specify which encryption method is used for encrypted communication with the user.

Console path:

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

Possible values:

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)

2.9.32.9 Privacy-Password

Enter the user password necessary for encryption here.

Cleartext input is only possible if the parameter in *2.9.32.15 Privacy-Password-Type* on page 25 was changed.

Console path:

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

Possible values:

Max. 130 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

empty

2.9.32.13 Status

Activates or deactivates this user.

Console path:

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

Possible values:

Active
inactive

Default:

Active

2.9.32.14 Authentication-Password-Type

The password in *2.9.32.6 Authentication-Password* on page 24 is always stored in encrypted format (type “Masterkey”). If you wish to enter a new password, for example from the command-line interface, you must first change the type to “Plaintext” here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to “Masterkey”.

Console path:

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

Possible values:

Plaintext
Masterkey

2.9.32.15 Privacy-Password-Type

The password in *2.9.32.9 Privacy-Password* on page 24 is always stored in encrypted format (type “Masterkey”). If you wish to enter a new password, for example from the command-line interface, you must first change the type to “Plaintext” here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to “Masterkey”.

Console path:

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

Possible values:

Plaintext
Masterkey

2.9.34 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.

Console path:

Setup > **SNMP**

2.9.34.1 Name

Specify the target address name here.

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

2.9.34.3 Transport-Address

The transport 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.

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

2.9.34.7 Parameters-Name

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

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

2.9.34.9 Status

Activates or deactivates this target address.

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

Active
inactive

Default:

Active

2.9.35 Target-Params

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

Console path:

Setup > **SNMP**

2.9.35.1 Name

Give the entry a descriptive name here.

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

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

Default:

empty

2.9.35.2 Message-Processing-Model

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

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

SNMPv1
SNMPv2c
SNMPv3

Default:

SNMPv3

2.9.35.3 Security-Model

Use this entry to specify the security model.

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default:

SNMPv3_USM

2.9.35.4 Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

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

Default:

empty

2.9.35.5 Security-Level

Set the security level that applies for the recipient to receive the SNMP traps

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

NoAuthNoPriv

The SNMP message 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.

AuthNoPriv

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

AuthPriv

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.

Default:

NoAuthNoPriv

2.9.35.7 Status

Activates or deactivates this entry.

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

Active
inactive

Default:

Active

2.9.37 Admitted-Protocols

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

Console path:

Setup > **SNMP**

Possible values:

SNMPv1
SNMPv2
SNMPv3

Default:

SNMPv3

2.9.38 Allow-Admins

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

Console path:

Setup > **SNMP**

Possible values:

No
Yes

Default:

No

2.9.41 Operating

This entry enables or disables SNMP traps.

Console path:

Setup > **SNMP**

Possible values:

No
SNMP traps are switched off.
Yes
SNMP traps are enabled.

Default:

No

2.11 Config

Contains the general configuration settings.

Console path:

Setup

2.11.1 Comment-1

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.2 Comment-2

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.3 Comment-3

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.4 Comment-4

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.11.5 Comment-5

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.11.6 Comment-6

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.11.7 Comment-7

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.11.8 Comment-8

Comment on this device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.9 Location

Location of the device. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.10 Administrator

Name of the device administrator. For display purposes only.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.11 Config-Aging-Minutes

Specify here the number of minutes after which an inactive TCP configuration connection (e.g. via SSH) is automatically terminated.

Console path:

Setup > **Config**

Possible values:

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

Default:

15

2.11.18 LED-Mode

Set the operating mode for the LEDs.

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

Console path:

Setup > **Config**

Possible values:

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 will shut off after a configurable time (**LED-Off-Seconds**).

Default:

On

2.11.20 Cron-Table

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.

Console path:

Setup > **Config**

2.11.20.1 Index

Used to sort multiple Cron jobs.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

max. 5 Zeichen aus `[0-9]`

2.11.20.2 Active

Determines whether the job is executed.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Yes
No

2.11.20.3 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.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Real-Time
Operating-Time

2.11.20.4 Minute

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

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 59 (1,2,3 or 0-59 or 1-3,59)`

2.11.20.5 Hour

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

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 23 (1,2,3 or 0-23 or 1-3,23)`

2.11.20.6 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.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 6 (1,2,3 or 0-6 or 1-3,6)`

2.11.20.7 Day

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

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 32 characters from `Range or comma-separated list between 1 and 31 (1,2,3 or 1-7 or 1-3,7,8-9)`

2.11.20.8 Month

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

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 32 characters from `Range or comma-separated list between 1 and 12 (1,2,3 or 1-7 or 1-3,7,8-9)`

2.11.20.9 Command

The CLI command to be executed.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

2.11.20.10 Comment

A free-text field for entering any comment.

Console path:

Setup > **Config** > **Cron-Table**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.21 Admins

Use this table to create administrators with restricted rights.

The root administrator always has all rights.

Console path:

Setup > **Config**

2.11.21.1 Administrator

Login name of the administrator in this row of the table.

Console path:

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

Possible values:

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

2.11.21.3 Function-Rights

Here you activate the administrator's function rights in this row of the table.

Console path:

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

Possible values:

Basic
Admin-Management

2.11.21.5 Rights

The rights of the administrator in this row of the table.

Console path:

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

Possible values:

None
Admin-RO-Limit
Admin-RW-Limit
Admin-RO
Admin-RW
Supervisor

2.11.21.6 Hashed-Password

Hash value of the administrator password in this row of the table.

Console path:

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

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.11.50 LL2M

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. In these cases, the only help is to reset the device to its factory default settings. This option requires physical access to the device, which may not always be possible with concealed access point installations and may mean a considerable overhead for large-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 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 *1.6 Command-line interface — command summary* on page 9.

You must have root rights on the LL2M server to run commands on the LL2M client.

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).

The menu contains the settings for R&S®NC layer 2 management.

Console path:

Setup

2.11.50.1 Operating

Enables/disables the LL2M server.

Console path:

Setup > **LL2M**

Possible values:

No

LL2M server is disabled.

Yes

LL2M server is enabled.

Default:

Yes

2.11.50.2 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. Access via WLAN is not planned.

Console path:

Setup > **LL2M**

2.11.50.2.1 Port

Port designation, e.g. ETH1.

Console path:

Setup > **LL2M** > **Interfaces**

Possible values:

Max. 5 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.11.50.2.2 Active

Enables/disables the LL2M server on this port.

Console path:

Setup > **LL2M** > **Interfaces**

Possible values:

No
Yes

Default:

Yes

2.11.51 Tacacs-Plus

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

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.

Console path:

Setup > **Config**

2.11.51.1 Operating

Switches the use of TACACS+ on or off.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

No
TACACS+ mode is switched off.

Yes
TACACS+ mode is switched on.

Default:

No

2.11.51.2 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.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

No
Authentication fallback is switched off.

Yes
Authentication fallback is switched on.

Default:

Yes

2.11.51.10 Server-Address

The IP address of the primary TACACS+ server.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

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

Default:

empty

2.11.51.11 Server-Port

The port of the primary TACACS+ server.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

0 … 65535

Default:

49

2.11.51.12 Server-Secret

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

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

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

Default:

empty

2.11.51.20 Spare-Server-Address

The IP address of the backup TACACS+ server.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

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

Default:

empty

2.11.51.21 Spare-Server-Port

The port of the backup TACACS+ server.

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

0 … 65535

Default:

49

2.11.51.22 Spare-Server-Secret

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

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

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

Default:

empty

2.11.52 SSH

Configure SSH settings here.

Console path:

Setup > **Config**

2.11.52.1 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.

Console path:

Setup > **Config** > **SSH**

Possible values:

2048 Bits (2048)
4096 Bits (4096)

Default:

2048 Bits (2048)

2.11.52.5 Keys

In addition to interactive authentication using a user name and password, public key authentication can also be used. You can configure it here.

Console path:

Setup > **Config** > **SSH**

2.11.52.5.1 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 *2.11.21 Admins* on page 37).

Console path:

Setup > **Config** > **SSH** > **Keys**

Possible values:

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

2.11.52.5.2 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.

Console path:

Setup > **Config** > **SSH** > **Keys**

Possible values:

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

2.11.52.5.3 Algo

The algorithm used to generate the public key.

Console path:

Setup > **Config** > **SSH** > **Keys**

Possible values:

ssh-rsa
ssh-dss
ssh-ed25519
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
rsa-sha2-256
rsa-sha2-512
sk-ecdsa-sha2-nistp256-openssh
sk-ssh-ed25519-openssh

2.11.52.5.4 Key

The public key to be used.

Console path:

Setup > **Config** > **SSH** > **Keys**

Possible values:

Max. 1400 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.11.90 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**.

Console path:

Setup > **Config**

Possible values:

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

Default:

300

2.11.91 LED-Test

This can be used to test the device LED. It will then illuminate in the corresponding color.

Console path:

Setup > **Config**

Possible values:

Off
Red
Green
Blue
All
No-Test

Default:

No-Test

2.11.99 Root-Hashed

Hash value of the password of the root administrator.

Console path:

Setup > **Config**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.11.130 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.

Console path:

Setup > **Config**

Possible values:

No

The PoE Passthrough feature is turned off.

Yes

The PoE Passthrough feature is turned on.

Default:

No

2.14 Time

Contains the general configuration settings for the time setting.

Console path:

Setup

2.14.15 Holidays

In this table, configure the public holidays for use in timeframes, for example.

Console path:

Setup > **Time**

2.14.15.1 Date

In this table, configure the public holidays for use in timeframes, for example.

Console path:

Setup > **Time** > **Holidays**

Possible values:

Max. 10 characters from `mm/dd/yyyy`

Special values:

yyyy = 0

Represents any year.

2.14.16 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.

Console path:

Setup > **Time**

2.14.16.1 Name

Enter the name of the time frame for referencing from the logical WLAN settings.

Console path:

Setup > **Time** > **Timeframe**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.14.16.2 Home

Here you set the start time (time of day) in the format HH:MM when the selected profile becomes valid.

Console path:

Setup > **Time** > **Timeframes**

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

2.14.16.3 Stop

Here you set the end time (time of day) in the format HH:MM when the selected profile ceases to be valid.

A stop time 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.

Console path:

Setup > **Time** > **Timeframes**

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

2.14.16.4 Weekdays

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

Console path:

Setup > **Time** > **Timeframes**

Possible values:

None
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Holiday

All days specified in the table *2.14.15 Holidays* on page 46.

2.14.20 Timezone

Configure the time zone for the location of the device.

Console path:

Setup > **Time**

Possible values:

UTC
Europe/Berlin
Europe/Vienna
Europe/Zurich
Europe/London
Europe/Prague
Europe/Warsaw
Europe/Zagreb
Europe/Copenhagen
Europe/Paris
Europe/Helsinki
Europe/Tallinn
Europe/Athens
Europe/Budapest
Europe/Dublin
Europe/Rome
Europe/Riga
Europe/Vilnius
Europe/Luxembourg
Europe/Malta
Europe/Amsterdam
Europe/Nicosia
Europe/Lisbon
Europe/Bucharest
Europe/Bratislava
Europe/Ljubljana
Europe/Madrid
Europe/Stockholm
Europe/Brussels
Europe/Sofia
US/Alaska
US/Pacific
US/Mountain
US/Central
US/Eastern
Pacific/Auckland
Pacific/Honolulu
Australia/Brisbane
Australia/Sydney
Australia/Perth
Australia/Darwin
Australia/Adelaide

Default:

UTC

2.14.21 NTP

Use this menu to configure an NTP server.

Console path:

Setup > **Time**

2.14.21.1 Operating

Enable the configured NTP server.

Console path:

Setup > **Time** > **NTP**

Possible values:

No

Do not use an NTP server.

Yes

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

Default:

No

2.14.21.1 Server

Enter the address of the NTP server.

Console path:

Setup > **Time** > **NTP**

Possible values:

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

Default:

empty

2.20 WLAN

Configuration settings for the WLAN parameters

Console path:

Setup

2.20.1 Network

Here you configure the general settings for the WLAN networks (SSIDs) that are broadcast. Add a line to the table for each WLAN network. By default, the table is empty.

Console path:

Setup > **WLAN**

2.20.1.1 Network-Name

Configure 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.2 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.4 Closed-Network

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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Show SSID.

Yes

Do not show SSID.

2.20.1.10 Max-Stations

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

0 … 512

Special values:

0

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).

2.20.1.13 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 *2.20.1.14 Client-Isolation* on page 52 has to be configured.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Communication between the WLAN clients on the WLAN network is not permitted.

Yes

Communication between the WLAN clients on the WLAN network is permitted.

2.20.1.14 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 here for each SSID. Enter the allowed destinations under *2.20.5 Client-Isolation-Allowed* on page 78.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

No client isolation.

Yes

Client isolation is active for this network.

2.20.1.16 Min-Client-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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

0 … 100

Special values:

0

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

2.20.1.17 Exclude-From-Client-Management

Excludes this SSID from the band steering if necessary.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Perform band steering with this SSID.

Yes

Exclude SSID from the band steering.

2.20.1.18 Timeframe

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.20.1.19 Hotspot

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

Default:

empty

2.20.1.20 Summaric-Tx-Limit-Kbit/s

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 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

Special values:

0

The value “0” means that no limitation is active.

2.20.1.21 Summaric-Rx-Limit-Kbit/s

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 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

Special values:

0

The value “0” means that no limitation is active.

2.20.1.25 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Do not block multicasts.

IPv4-only

Block IPv4 multicasts only.

IPv6-only

Block IPv6 multicasts only.

Both

Block both IPv4 and IPv6 multicasts.

Default:

No

2.20.1.26 Client-Tx-Limit-Kbit/s

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.27 Client-Rx-Limit-Kbit/s

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.28 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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.

Default:

Off

2.20.1.29 Multicast-To-Unicast

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

None
Conversion

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.

Encapsulation

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.

2.20.1.30 Bridge

Used internally in WLC mode or when operating L2TP, the L2TP interface must be entered here.

Console path:

Setup > **WLAN** > **Network**

Possible values:

br-lan
WLC-Tunnel-1 … WLC-Tunnel-32
L2TP-Tunnel-1 … L2TP-Tunnel-16

2.20.1.32 WDS link

Here you choose to broadcast specific SSIDs over WDS links. Also see *2.20.13.1.1 Link-Name* on page 92.

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.34 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Unscheduled APSD deactivated.

Yes

Unscheduled APSD activated.

Default:

Yes

2.20.1.35 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Radio Resource Measurement disabled.

Yes

Radio Resource Measurement enabled.

2.20.1.36 DTIM-Period

The DTIM period can be configured via SSID.

Console path:

Setup > **WLAN** > **Network**

Possible values:

1 … 255

Default:

1

2.20.1.42 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.

Console path:

Setup > **WLAN** > **Network**

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.

2.20.1.43 Client-Mgmt-Profile

Select one of the Client Management profiles from *2.20.18.2 Profiles* on page 100 here.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.100 Key

Configure the pre-shared key (PSK) used for the WLAN network here.

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, LANCOM Systems 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

Console path:

Setup > **WLAN** > **Network**

Possible values:

8 to 63 characters `WPA key`

2.20.1.101 Radios

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

Console path:

Setup > **WLAN** > **Network**

Possible values:

2.4GHz+5GHz
The SSID is broadcast on the frequencies 2.4 GHz and 5 GHz.

2.4GHz
The SSID is only broadcast on the 2.4-GHz frequency.

5GHz
The SSID is only broadcast on the 5-GHz frequency.

None
The SSID will not be broadcast. This can be used as a general on/off switch for the SSID.

2.20.1.102 Encryption-Profile

Here you configure an encryption profile from the methods available under **Setup** > **WLAN** > **Encryption**. This profile defines which authentication and encryption method should be used for the SSID.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.103 Idle-Timeout

This is the time in seconds after which a client is disconnected if the access point has no more packets received from it. Any traffic from the client resets this timeout.

Console path:

Setup > **WLAN** > **Network**

Possible values:

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

2.20.1.200 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.

Console path:

Setup > **WLAN** > **Network**

Possible values:

0 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

2.20.2 Country

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

Console path:

Setup > **WLAN**

Possible values:

Australia
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech-Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
New-Zealand
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United-Kingdom
United-States
Europe

2.20.3 Encryption

Here you configure the settings for the encryption and authentication on the WLAN networks. A variety of encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

Console path:

Setup > **WLAN**

2.20.3.1 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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

2.20.3.2 Encryption

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

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No

Do not use encryption.

Yes

Use encryption.

2.20.3.4 Method

Here you configure the encryption method.

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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

WEP-40-Bits

AES with 40 bits key length

WEP-104-Bits

AES with 104 bits key length

WEP-128-Bits

AES with 128 bits key length

WEP-40-Bits-802.1X

AES 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

AES 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

AES with 128 bits key length and 802.1X

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

802.11i-WPA-PSK

WPA(2) with Pre-Shared-Key

802.11i-WPA-802.1X-192-Bits

WPA(2) with 802.1X and 192 bits key length

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.

2.20.3.9 WPA-Version

Here you configure the WPA version used for the encryption methods **802.11i WPA-PSK** and **802.11i WPA 802.1X**.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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.

2.20.3.11 WPA-Rekeying-Cycle

Here you configure the time in seconds after which the access point performs rekeying when operating WPA(2).

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

Max. 32 characters from `[0-9]`

Special values:

0

The value “0” means that no rekeying is performed.

2.20.3.12 WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used.

Operating TKIP is only recommended when using 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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.

2.20.3.13 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.

Operating TKIP is only recommended when using 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.

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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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.

Default:

AES-CCMP-128

2.20.3.14 Prot.-Mgmt-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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No
Do not use PMF.

optional
Offer PMF. The client decides whether to use them.

mandatory
Use PMF

2.20.3.15 Prot.-Beacons

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

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No
Beacon Protection switched off.

Yes
Beacon Protection switched on.

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

Default:

Auto

2.20.3.16 Pre-Authentication

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

Usually, a WLAN client carries out a background scan of the environment to find existing APs that it could connect to. APs 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 AP via the infrastructure network, which interconnects the APs. 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 AP 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 AP 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 AP, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the PMK caching.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No

Do not perform pre-authentication.

Yes

Perform pre-authentication.

2.20.3.17 OKC

This option enables or disables the Opportunistic Key Caching (OKC).

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No

OKC is enabled.

Yes

OKC is not enabled.

2.20.3.19 WPA2-Key-Management

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

Console path:

Setup > **WLAN** > **Encryption**

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.

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.

2.20.3.20 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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

2.20.3.21 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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

2.20.3.26 SAE/OWE-Groups

Contains the selection of the available Diffie-Hellman groups as a bit mask 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

DH-19
Bit 0x80000 (524288) – 256-bit random ECP group

DH-20
Bit 0x100000 (1048576) – 384-bit random ECP group

DH-21
Bit 0x200000 (2097152) – 521-bit random ECP group

Default:

DH-19

2.20.4 Band-Steering

Configure the settings for band steering here. Using band steering, clients can be steered from the overloaded 2.4-GHz frequency band to the 5-GHz frequency band, so that more bandwidth is available for the individual client, and the user experience is improved. LCOS LX supports 802.11v standard, which has the option to steer clients to the frequency band that offers them the best signal. Even clients that do not support the 802.11v standard can be steered to the 5-GHz band by deliberately delaying probe responses or by deliberately disconnecting them from the WLAN.

Console path:

Setup > **WLAN**

2.20.4.1 Active-Profile

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

Console path:

Setup > **WLAN** > **Band-Steering**

Possible values:

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

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

<Custom>

In addition to the existing profiles, you can also define your own profiles under **Profiles**.

Default:

P-DEFAULT

2.20.4.2 Profiles

Here you adjust the detailed settings of the steering profiles or you can create a new profile.

Console path:

Setup > **WLAN** > **Band-Steering**

2.20.4.2.1 Profile-Name

The name of the profile.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.2 Operating

Controls whether band steering is active for this profile.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

No

Band steering is not active.

Yes

Band steering is active.

2.20.4.2.3 Steering-Min-PHY-Signal

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

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.4 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.5 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.6 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.7 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.8 2.4GHz-Sub-Profile

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

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.2.9 5GHz-Sub-Profile

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

Console path:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Possible values:

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

2.20.4.3 2.4GHz-Sub-Profiles

Configure the settings of the 2.4-GHz sub-profile here.

Console path:

Setup > **WLAN** > **Band-Steering**

2.20.4.3.1 Profile-Name

The profile name of the 2.4-GHz sub-profile.

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

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

2.20.4.3.2 Utilization-Check-Interval

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

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

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

2.20.4.3.3 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

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

2.20.4.3.4 Utilization-Overload-Threshold

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

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

0 … 100

2.20.4.3.5 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).

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

0 … 100

2.20.4.3.6 Interference-Detection

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

Console path:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:

No
Do not take interference into account.

Yes
Take interference into account.

2.20.4.3.7 Delay-Probe-PHY-Signal-Threshold

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

Console path:
Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:
Max. 10 characters from `[0-9]`

2.20.4.3.8 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 probe min. request count** before it responds to them.

Console path:
Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:
Max. 10 characters from `[0-9]`

2.20.4.3.9 Delay-Probe-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.

Console path:
Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Possible values:
Max. 10 characters from `[0-9]`

2.20.4.4 5GHz-Sub-Profiles

Configure the settings of the 5-GHz sub-profile here.

Console path:
Setup > **WLAN** > **Band-Steering**

2.20.4.4.1 Profile-Name

The profile name of the 5-GHz sub-profile.

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

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

2.20.4.4.2 Utilization-Check-Interval

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

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

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

2.20.4.4.3 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.

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

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

2.20.4.4.4 Utilization-Overload-Threshold

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

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

0 … 100

2.20.4.4.5 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).

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

0 … 100

2.20.4.4.6 Interference-Detection

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

Console path:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Possible values:

No

Do not take interference into account.

Yes

Take interference into account.

2.20.5 Client-Isolation-Allowed

Configure the allowed destinations for client isolation here. See also *2.20.1.14 Client-Isolation* on page 52.

Console path:

Setup > **WLAN**

2.20.5.1 Network-Name

Select the network / SSID that the entry should apply for. Then enter either a destination IP address (*2.20.5.2 IP network* on page 79) or destination MAC (*2.20.5.3 MAC-Address* on page 79) 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.

Console path:

Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

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

2.20.5.2 IP network

Allowed destination IP address for this network.

Console path:

Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

Max. 19 characters of an IPv4 address `a.b.c.d/xx`

2.20.5.3 MAC-Address

Allowed destination MAC address for this network.

Console path:

Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

Max. 17 characters of a MAC address `xx:xx:xx:xx:xx:xx`

2.20.8 Radio-Settings

Here you configure all of the settings relating to the physical radio parameters. By default, there is an entry in the table for every physical WLAN radio for modification as required.

Console path:

Setup > **WLAN**

2.20.8.1 Ifc

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

Console path:

Setup > **WLAN** > **Radio-Settings**

2.20.8.3 5GHz-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:

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

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

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.

Auto
All modes supported by the device are used.

2.20.8.6 Radio-Band

Here you configure whether this radio module works in the 2.4-GHz, 5-GHz or 6-GHz spectrum.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

2.4GHz
The radio module works in the 2.4-GHz spectrum.

5GHz
The radio module works in the 5-GHz spectrum.

6GHz
The radio module works in the 6-GHz spectrum.

2.20.8.7 Sub-Band

Here you configure which sub-bands are used in the 5-GHz mode.

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

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

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

Sub-bands 1 and 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).

2.20.8.8 Channel

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

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 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.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

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

Special values:

0

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.

2.20.8.9 2.4GHz-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.

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

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

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.

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

2.20.8.13 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.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

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

2.20.8.17 Antenna-Mask

Only devices with external or detachable antennas have the antenna mask settings.

This setting helps when using WLAN antennas with a different number of streams from the access point (e.g. antenna with two streams, connected to an access point with four streams). This can be used to deactivate the ports on the access point side that are not connected to an antenna.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

All (0x0)
If no bit of this mask is set, then all antennas are active.

Antenna-1 (0x1)
Bit 1 controls antenna 1.

Antenna-2 (0x2)
Bit 2 controls antenna 2.

Antenna-3 (0x4)
Bit 3 controls antenna 3.

Antenna-4 (0x8)
Bit 4 controls antenna 4.

Default:

All (0x0)

2.20.8.19 6GHz-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:

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

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

11ax
The mode 802.11ax (Wi-Fi 6) is used.

11axbe-mixed
The modes 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) are used.

Auto
All modes supported by the device are used.

2.20.8.24 Max.-Channel-Bandwidth

Here you configure the maximum allowed channel bandwidth.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

20MHz
The channel bandwidth is always 20 MHz.

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

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

160MHz
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.

320MHz
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.

Auto
For a 2.4-GHz radio the channel bandwidth of 20 MHz is 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 160 MHz) is used.

2.20.8.29 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**.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

No
Use channels reserved for DFS.

Yes
Do not use channels reserved for DFS.

2.20.8.33 Power-Setting

This setting regulates whether to use the maximum permitted transmission power supported by the hardware of the access point (“Automatic”) or whether the desired target transmission power can be specified in the manual mode (“Manual”). This is done in dBm under *2.20.8.34 EIRP* on page 85.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Automatic

Use the maximum permitted transmission power that can be realized by the hardware of the access point.

Manual:

Use the target transmission power specified in dBm under *2.20.8.34 EIRP* on page 85.

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.

Default:

Automatic

2.20.8.34 EIRP

Depending on the setting in *2.20.8.33 Power-Setting* on page 84, 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.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Max. 2 characters from `[0-9]`

2.20.8.35 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.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Yes
Use channels reserved for weather radar.

No
Do not use channels reserved for weather radar.

2.20.8.36 Max.-Distance

Enter the distance to the most distant WLAN station here (e.g., to a WDS partner).

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

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Max. 2 characters from `[0-9]`

Default:

1

2.20.8.37 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 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.

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Auto
Automatic channel selection.

Random
Random WLAN channel selection.

2.20.9 Automatic-Environment-Scan-Enabled

This entry is set by the R&S®LANCOM Management Cloud, which requires the environment scan. The results can only be read by the R&S®LANCOM Management Cloud.

Console path:

Setup > **WLAN**

Possible values:

Yes

Automatic environmental scan is performed.

No

Automatic environmental scan is not performed.

2.20.10 Automatic-Environment-Scan-Time-Begin

Start time for the time window in which the automatic environmental scan is performed.

Console path:

Setup > **WLAN**

Possible values:

Time in format `hh:mm`

2.20.11 Automatic-Environment-Scan-Time-End

Stop time for the time window in which the automatic environmental scan is performed.

Console path:

Setup > **WLAN**

Possible values:

Time in format `hh:mm`

2.20.12 Hotspot

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN**

2.20.12.1 Hotspots

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot**

2.20.12.1.1 Name

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

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

2.20.12.1.2 URL

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

Max. 256 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.12.1.3 Revision-ID

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

Max. 36 characters from `UUID`

2.20.12.1.4 Private-Network

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

No
Yes

2.20.12.1.5 DHCP-Range-Start

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

Max. 32 characters from `IPv4 address: a.b.c.d`

2.20.12.1.6 DHCP-Range-End

This is an internal value of the cloud-managed hotspot feature managed by the R&S®LANCOM Management Cloud. It must not be changed.

Console path:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Possible values:

Max. 32 characters from `IPv4 address: a.b.c.d`

2.20.12.2 Walled-Garden

Walled Garden allows you to define IP addresses or hostnames that should be reachable for hotspot clients who are not yet logged in. Typically, these are hosts that provide additional resources required by the landing page (e.g., graphics, fonts, or even entire third-party login services).

To configure the Walled Garden, proceed as follows:

1. Create a Cloud-managed Hotspot in the R&S®LANCOM Management Cloud.
2. Next, determine the name of this Cloud-managed Hotspot from the table under **Setup** > **WLAN** > **Hotspot** > **Hotspots**.
3. Now create one or more entries in this table, with “Hotspot” containing the name of the hotspot configuration and “Hostname” containing the host or IP address to be allowed. The use of wildcards such as “*.lancom.de” is possible.
4. If a Walled Garden host should only be accessible without login when the R&S®LANCOM Management Cloud is not reachable, then for each entry the switch “LMC-unreachable-only” can additionally be set.
5. Finally, save the configuration using the command “flash”.

DNS requests from unauthenticated clients in the hotspot network are analyzed, and the resolved IP addresses are cached in the background to support the use of wildcards.

To simplify the process, it is recommended to perform these configuration steps in the R&S®LANCOM Management Cloud using an add-in.

Console path:

Setup > **WLAN** > **Hotspot**

2.20.12.2.1 Hotspot

Name of the hotspot.

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

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

2.20.12.2.2 Hostname

Enter here the host to be enabled or its IP address. The use of wildcards such as “*.lancom.de” is possible.

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-*`

2.20.12.2.3 LMC-unreachable-only

If a Walled Garden host should only be accessible without login when the R&S®LANCOM Management Cloud is not reachable, this switch can additionally be set to “Yes”.

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

No
Yes

2.20.12.3 Allowed-Targets

In networks operated as a Cloud-managed Hotspot, traffic to RFC1918 networks is generally prohibited. This affects the following networks:

- 10.0.0.0/8
- 192.168.0.0/16

› 172.16.0.0/12

With this feature, traffic to these networks or to individual hosts can be selectively allowed.

An add-in is required in the R&S®LANCOM Management Cloud.

Console path:

Setup > **WLAN** > **Hotspot**

2.20.12.3.1 Hotspot

Name of the hotspot.

Console path:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

Possible values:

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

2.20.12.3.1 IP-Network

Allowed IPv4 network for this hotspot.

Console path:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

Possible values:

Max. 19 characters from `IPv4 address: a.b.c.d/xx`

2.20.13 WDS

The Wireless Distribution System (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).

Console path:

Setup > **WLAN**

2.20.13.1 Links

In this table you configure the general settings for the WLAN networks (SSIDs) that are broadcast. Add a line to the table for each WLAN network. By default, the table is empty.

Console path:

Setup > **WLAN** > **WDS**

2.20.13.1.1 Link-Name

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

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

2.20.13.1.2 SSID name

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

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

2.20.13.1.3 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.

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

Access point
Station

2.20.13.1.4 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).

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

2.4GHz
The SSID is only broadcast on the 2.4 GHz frequency.

5GHz
The SSID is only broadcast on the 5 GHz frequency.

6GHz
The SSID is only broadcast on the 6 GHz frequency.

2.20.13.1.5 Encryption-Profile

The encryption profile to be used for the WDS link.

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

2.20.13.1.6 Encryption-Key

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

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

2.20.13.1.8 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]).

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

Max. 128 characters from `[0-9],`

2.20.13.1.9 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.

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

No
Yes

Default:

Yes

2.20.13.1.10 Additional-Untagged-VLAN

Non-VLAN tagged packets are transmitted via the WDS link.

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

No
Non-VLAN tagged packets are not transmitted via the WDS link.

Yes
Non-VLAN tagged packets are transmitted via the WDS link.

Default:

Yes

2.20.13.1.11 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.

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first.

If required, create a roaming profile.

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

2.20.13.2 Encryption

The settings for encryption and authentication of the Wireless Distribution System are configured in this table.

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

Console path:

Setup > **WLAN** > **WDS**

2.20.13.2.1 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.

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

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

2.20.3.2.2 Method

Here you configure the encryption method.

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

802.11i-WPA-PSK

WPA(2/3) with Pre-Shared-Key

2.20.13.2.3 WPA version

Here you configure the WPA version used for the encryption methods **802.11i WPA-PSK** and **802.11i WPA 802.1X**.

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

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.

2.20.13.2.4 WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used.

Operating TKIP is only recommended when using 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.

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

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.

2.20.13.2.5 WPA2 session keytypes

Here you configure the session key type to be used for WPA version 2 or 3. This also influences the encryption method used.

Operating TKIP is only recommended when using 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.

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

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.

2.20.13.2.6 RADIUS-Client-Profile

Specify a RADIUS client profile here if necessary.

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

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

2.20.13.3 Roaming

Configure the settings for the roaming profile here.

Console path:

Setup > **WLAN** > **WDS**

2.20.13.3.1 Profile-Name

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

Console path:

Setup > **WLAN** > **WDS** > **Roaming**

Possible values:

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

2.20.13.3.2 Signal-Strength-Threshold

Enter here 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.

Console path:

Setup > **WLAN** > **WDS** > **Roaming**

Possible values:

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

2.20.13.3.3 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.

Console path:

Setup > **WLAN** > **WDS** > **Roaming**

Possible values:

0 … 4,294,967,295 Seconds

2.20.13.3.4 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.

Console path:

Setup > **WLAN** > **WDS** > **Roaming**

Possible values:

0 … 4,294,967,295 Seconds

2.20.14 Include-UUID

Configures whether an access point transmits its UUID. The LANCOM UUID is used, among other things, as an Ekahau extension for combining multiple SSIDs into one access point.

Console path:

Setup > **WLAN**

Possible values:

No
UUID not transferred.

Yes
UUID transferred.

Default:

No

2.20.15 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.

Console path:
Setup > **WLAN**

Possible values:

No
WLAN power-saving mode off.

Yes
WLAN power-saving mode on.

Default:

No

2.20.16 Include-Devicename

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
```

Console path:

Setup > **WLAN**

Possible values:

No

Do not transfer device names.

Yes

Transfer device name.

Default:

No

2.20.18 Client-Management

Configure client management here.

Console path:

Setup > **WLAN**

2.20.18.2 Profiles

Define configuration profiles for client management here. You can select the profiles in the network table.

Console path:

Setup > **WLAN** > **Client-Management**

2.20.18.2.1 Profile-Name

Name of this profile.

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

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

2.20.18.2.2 RRM

Enable the use of RRM here.

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

No
Yes

2.20.18.2.3 BTM

Enable the use of WNM/BTM here.

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

No
Yes

2.20.18.2.4 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.

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

0 … 100

2.20.18.3 Radio-Settings

Define the radio settings for client management here.

Console path:

Setup > **WLAN** > **Client-Management**

2.20.18.3.1 Ifc

The WLAN interface to which the following settings apply.

Console path:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Possible values:

Max. 9 characters from `WLAN-1,WLAN-1-2,...`

2.20.18.3.2 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.

Console path:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Possible values:

0 … 100

2.20.18.3.3 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.

Console path:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Possible values:

0 … 100

2.20.19 Client-Management-Mode

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

Console path:

Setup > **WLAN**

Possible values:

Client-Management
Band-Steering
Off

2.20.20 End2End-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.

Console path:

Setup > **WLAN**

2.20.20.1 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.1.1 Profile-Name

The name of this test profile.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.2 WLAN-Connection

Select one of the available WLAN connections.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.3 WLAN-Authentication

Select one of the available WLAN authentication configurations.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.4 IPv4-Mode

Select either DHCP or Static.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

DHCP
Static

2.20.20.1.5 IPv6-Mode

Select either Router Advertisement, DHCPv6, Static, or Off.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

Router-Advertisement
DHCPv6
static
Off

2.20.20.1.6 IPv4-Static-Parameters

If required, select the static IPv4 parameters.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.7 IPv6-Static-Parameters

If required, select the static IPv6 parameters.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.8 DNS-Targets

Select one of the available DNS targets.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.9 Ping-Targets

Select one of the available ping targets.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.10 Captive-Portal-Login

Select one of the available captive portal logins.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

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

2.20.20.1.11 HTTP-Targets

Select one of the available HTTP targets.

Console path:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.2 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.2.1 WLAN-Connection-Name

Enter a name for this connection.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Possible values:

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

2.20.20.2.2 SSID-Name

The SSID for the tests.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Possible values:

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

2.20.20.2.3 BSSID

Optional BSSID for the tests.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Possible values:

Max. 17 characters from `mac address (xx:xx:xx:xx:xx:xx)`

2.20.20.2.4 Radio-Band

The radio band for this connection.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Possible values:

2.4GHz
5GHz
6GHz

2.20.20.3 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.3.1 WLAN-Authentication-Name

Enter a name for this WLAN authentication configuration.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

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

2.20.20.3.2 Encryption-Key

Enter the PSK.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

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

2.20.20.3.3 Method

Select the WLAN authentication method.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

802.11i-WPA-PSK
802.11i-WPA-802.1X
Enhanced-Open
802.11i-WPA-802.1X-192-Bits

2.20.20.3.4 WPA-Version

Select the WPA version.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

WPA1
WPA2
WPA1/2
WPA3
WPA2/3

2.20.20.3.5 Session-Keytypes

Select the session key type.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

TKIP
AES
TKIP/AES

2.20.20.3.6 802.1X-Client-Profile

Select an IEEE 802.1X client profile.

Console path:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Possible values:

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

2.20.20.4 IP-Static-Parameters

If a static IP configuration is to be used for the test, enter the corresponding IP parameters in this table.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.4.1 IP-Static-Parameters-Name

Enter a name for this static IP configuration.

Console path:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Possible values:

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

2.20.20.4.2 IP-Address

Enter the IP address.

Console path:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Possible values:

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

2.20.20.4.3 IP-Gateway

Enter the IP gateway.

Console path:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Possible values:

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

2.20.20.4.4 Primary-IP-DNS

Enter the IP address of the primary DNS server.

Console path:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Possible values:

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

2.20.20.4.5 Secondary-IP-DNS

Enter the IP address of the secondary DNS server.

Console path:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Possible values:

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

2.20.20.5 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.5.1 DNS-Targets-Name

Enter a name for this DNS target.

Console path:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Possible values:

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

2.20.20.5.2 DNS-Target-Hostname

Enter the hostnames to be tested.

Console path:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-`

2.20.20.5.3 Expected-Response

Enter the response expected for this test.

Console path:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Possible values:

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

2.20.20.6 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.6.1 Ping-Targets-Name

Enter a name for this ping target.

Console path:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Possible values:

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

2.20.20.6.2 Ping-Target-Hostname

Enter the hostname to be tested.

Console path:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-:%`

2.20.20.6.3 Ping-Count

Enter the number of pings.

Console path:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Possible values:

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

Default:

10

2.20.20.6.4 Fail-Count

Enter the number of failures.

Console path:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Possible values:

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

Default:

2

2.20.20.7 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.7.1 Captive-Portal-Login-Name

Enter a name for this captive portal login.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Possible values:

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

2.20.20.7.2 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.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Possible values:

Login
Logout

2.20.20.7.3 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.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.7.4 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.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.8 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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.8.1 HTTP-Targets-Name

Enter a name for this HTTP target.

Console path:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Possible values:

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

2.20.20.8.2 HTTP-Target-URL

Enter the URL to be tested.

Console path:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.8.3 Expected-Response

Enter the expected response.

Console path:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Possible values:

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

2.20.20.8.4 Max-Size-Bytes

Optional size limit.

Console path:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Possible values:

Max. 20 characters from `[0-9]`

2.20.20.9 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.

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.

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.20.9.1 Captive-Portal-Login-Name

Enter a name for this captive portal login.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Possible values:

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

2.20.20.9.2 Attribute

Enter the required attributes here.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` `

2.20.20.9.3 Value

Enter the values for the configured attributes here.

Console path:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` `

2.20.20.20 Run-Tests

Use this action to start the tests.

Example: `do Run-Tests`

Console path:

Setup > **WLAN** > **End2End-Test**

2.20.133 LEPS

R&S®NC Enhanced Passphrase Security (LEPS) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address. An alternative is to implement a MAC address filter.

Console path:

Setup > **WLAN**

2.20.133.1 Operating

Switches LEPS on or off. When switched off, LEPS users are ignored during WLAN client authentication.

Console path:

Setup > **WLAN** > **LEPS**

Possible values:

No
Yes

Default:

No

2.20.133.2 Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users. You can overwrite the profile values for any particular user with individual values.

Console path:

Setup > **WLAN** > **LEPS**

2.20.133.2.1 Name

Enter a unique name for the LEPS profile here.

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

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

2.20.133.2.2 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.

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

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

2.20.133.2.3 Mac-List

Here you specify if and how MAC addresses are checked.

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

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.

2.20.133.2.4 VLAN

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

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

0 … 4095

2.20.133.3 Users

Create individual LEPS users here. Every LEPS user must be connected to a profile that was created previously.

Console path:

Setup > **WLAN** > **LEPS**

2.20.133.3.1 Name

Enter a unique name for the LEPS user here.

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

2.20.133.3.2 Profiles

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.

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

2.20.133.3.3 WPA-Passphrase

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

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

2.20.133.3.4 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-ID configured for the LEPS user takes priority.

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

0 … 4095

2.20.133.3.7 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.

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

MAC address in the format `xx:xx:xx:xx:xx:xx`

2.20.1111 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. You can set the rates for the WLAN networks in this table.

Console path:

Setup > **WLAN**

2.20.1111.1 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 *2.20.1 Network* on page 51.

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

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

2.20.1111.23 Broadcast-Rate

The rate to use for sending broadcasts.

If 6 Mbit/s, 12 Mbit/s or 24 Mbit/s is selected as the broadcast rate, this rate is also used for sending beacons.

Rates other than these only affect broadcast packets and do not change the beacon rate.

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default:

default

2.20.1111.24 Multicast-Rate

The rate to use for sending multicasts.

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default:

default

2.20.1111.25 Beacon-Rate

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

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

default
6Mbps
12Mbps
24Mbps

Default:

default

2.20.1111.101 Radio-Band

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

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

2.4GHz+5GHz
2.4 GHz
5 GHz
None

Default:

2.4GHz+5GHz

2.22 Syslog

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

You can adjust the relevant settings here.

Console path:

Setup

2.22.2 Server

Configure one or more syslog servers in this 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.

Console path:

Setup > **Syslog**

2.22.2.1 Server

Name of the external syslog server.

Console path:

Setup > **Syslog** > **Server**

Possible values:

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

2.22.2.7 IP-Address

IP address of the external syslog server.

Console path:

Setup > **Syslog** > **Server**

Possible values:

Max. 64 characters from `IPv4 or IPv6 address`

2.22.2.8 Port

Port of the external Syslog server.

Console path:

Setup > **Syslog** > **Server**

Possible values:

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

Default:

514

2.22.2.9 Protocol

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

Console path:

Setup > **Syslog** > **Server**

Possible values:

TCP
UDP

Default:

TCP

2.23 Logging

Here you will find the settings for logging.

Console path:

Setup

2.23.1 Operating

Enables the trace system during the boot process.

If no entry is made in the table *2.23.5 Trace* on page 126, the trace system will automatically shut down.

Console path:

Setup > **Logging**

Possible values:

Yes

Trace system enabled.

No

Trace system not enabled.

Default:

No

2.23.2 Timer-Seconds

Indicates the number of seconds the system remains active. A value between 60 and 120 seconds is recommended, as experience shows that the lxcd typically takes that long to activate.

Console path:

Setup > **Logging**

Possible values:

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

Special values:

0

No time limit.

2.23.3 Level

This specifies which log level should be activated. A higher level automatically includes all lower levels. For example, selecting the Debug level would also activate the Error, Warning, and Info levels.

Console path:

Setup > **Logging**

Possible values:

Info

Level 0 - Info messages

Warning
Level 1 - Warnings
Error
Level 2 - Error messages
Debug
Level 3 - Debug messages
Guru
Level 4 - Messages for developers

Default:

Info

2.23.4 Target

This value indicates where the trace data will be written. If Syslog is selected, the active trace system will write messages to the Syslog.

Console path:
Setup > **Logging**

Possible values:

Syslog
Trace data will be written to Syslog. With remote Syslog, remote tracing would be possible here.
Devlog
Trace data will be written to /proc/lxlog. This log will be exported using the “Support Information” system.

Default:

Syslog

2.23.5 Trace

This table contains the names of the traces whose trace data should be written. You can get an overview of possible names using the CLI command `trace ?`.

Console path:
Setup > **Logging**

2.23.5.1 Name

A name in the trace table, whose trace data should be written. You can get an overview of possible names using the CLI command `trace ?`.

Console path:

Setup > **Logging** > **Trace**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]:*-_`

Default:

empty

2.23.6 Log-Persistence

This allows the last lxlog to be persisted after booting. When enabled, /tmp/lxlog_latest.gz will be copied to /config/lxbootlog.gz.

Console path:

Setup > **Logging**

Possible values:

Yes
No

Default:

No

2.30 RADIUS

Configuration settings of the parameters for RADIUS and IEEE 802.1X.

Console path:

Setup

2.30.3 RADIUS server

Here you configure the settings for RADIUS server profiles to be used with WLAN networks that operate 802.1X for authentication.

Console path:

Setup > **RADIUS**

2.30.3.1 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.

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

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

2.30.3.3 Port

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

This is usually the port 1812 (RADIUS authentication).

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

0 … 65535

2.30.3.4 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.

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

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

2.30.3.5 Backup

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

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

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

2.30.3.8 Server-IP-Address

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

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

Max. 64 characters from `IPv4 or IPv6 address`

2.30.3.9 Accounting port

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

This is usually the port 1813 (RADIUS accounting).

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

0 … 65535

2.30.3.14 Accounting IP address

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

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

Max. 64 characters from `IPv4 or IPv6 address`

2.30.3.15 MAC-Check

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

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

No

No check based on the MAC address.

Yes

Check the permissions of the clients on the RADIUS server by means of the MAC address.

2.30.3.16 Fallback-Dynamic-VLAN-ID

If no VLAN ID for a WLAN client is transmitted by a RADIUS server, the VLAN ID assigned here is used.

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

0 … 4095

Special values:

0

The default value 0 means that the VLAN ID sent by the RADIUS server is used.

2.30.3.17 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.

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

No

Message authenticator not required in RADIUS messages.

Yes

Message authenticator must be present in RADIUS messages.

2.30.4 Delete-WLAN-Supplicant-Certificates

With this action you delete all existing certificates of the WLAN supplicants.

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible arguments:

none

2.30.11 LAN-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.

Console path:

Setup > **RADIUS**

2.30.11.1 Interface name

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

Console path:

Setup > **RADIUS** > **LAN-Supplicant**

Possible values:

Max. 64 characters from `INTRANET`

2.30.11.2 Method

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

Console path:

Setup > **RADIUS** > **LAN-Supplicant**

Possible values:

None
MD5
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

2.30.11.3 User name

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

Console path:

Setup > **RADIUS** > **LAN-Supplicant**

Possible values:

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

2.30.11.4 Password

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

Console path:

Setup > **RADIUS** > **LAN-Supplicant**

Possible values:

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

2.30.12 WLAN-Supplicant

Here you will find the settings for the 802.1X supplicant functionality to authenticate the device WLAN-side to an infrastructure secured with 802.1X.

Console path:

Setup > **RADIUS**

2.30.12.1 Profile-Name

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

Console path:

Setup > **RADIUS** > **WLAN-Supplicant**

Possible values:

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

2.30.12.2 Method

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

Console path:

Setup > **RADIUS** > **WLAN-Supplicant**

Possible values:

none
MD5
TLS
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

2.30.12.3 Username

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

Console path:

Setup > **RADIUS** > **WLAN-Supplicant**

Possible values:

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

2.30.12.4 Password

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

Console path:

Setup > **RADIUS** > **WLAN-Supplicant**

Possible values:

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

2.30.12.5 Certificate

You can accept the RADIUS server certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server.

Console path:

Setup > **RADIUS** > **WLAN-Supplicant**

Possible values:

Auto-accept

Accept certificate automatically.

Container

Check uploaded certificate.

2.40 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.

Console path:

Setup

2.40.1 Operating

Turn multicast snooping on or off.

Console path:

Setup > **Multicast-Snooping**

Possible values:

No

Multicast snooping disabled.

Yes

Multicast snooping enabled.

2.45 Bridge

Console path:

Setup

2.45.1 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.

Console path:

Setup > **Bridge**

2.45.1.1 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.

The identifiers of the LAN ports can be viewed in the CLI table **Status** > **LAN** > **Ports**.

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

2.45.1.2 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.

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

2.45.1.3 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.

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

2.46 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.

Console path:

Setup

2.46.1 Services

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

Console path:

Setup > **mDNS-Filter**

2.46.1.1 Name

The name of a service.

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.46.1.2 Service-Type

The type of this service.

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.46.1.3 Comment

Comment for this entry.

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.46.2 Services-List

Configure filters here based on the services from the 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.

Console path:

Setup > **mDNS-Filter**

2.46.2.1 Network-Name

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

Console path:

Setup > **mDNS-Filter** > **Services-List**

Possible values:

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

2.46.2.2 Services

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

Console path:

Setup > **mDNS-Filter** > **Services-List**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.47 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.

Console path:

Setup

2.47.1 Rules

Configure the firewall rules here.

Console path:

Setup > **Firewall**

2.47.1.1 Enabled

Specifies whether the rule is active for the firewall.

Console path:

Setup > **Firewall** > **Rules**

Possible values:

No
Rule is inactive.

Yes
Rule is active.

2.47.1.2 Priority

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

Console path:
Setup > **Firewall** > **Rules**

Possible values:
Max. 10 characters from `[0-9]`

2.47.1.3 Network

The WLAN network for which the rule is active.

Console path:
Setup > **Firewall** > **Rules**

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

2.47.1.4 Host-Group

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

Console path:
Setup > **Firewall** > **Rules**

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

2.47.1.5 Protocol

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

Console path:
Setup > **Firewall** > **Rules**

Possible values:

Any
TCP
UDP

2.47.1.6 Port

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

Console path:

Setup > **Firewall** > **Rules**

Possible values:

0 … 65535

2.47.1.7 Action

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

Console path:

Setup > **Firewall** > **Rules**

Possible values:

Accept
Drop

2.47.1.99 Comment

A free-text field for entering any comment.

Console path:

Setup > **Firewall** > **Rules**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` `

2.47.2 Host-Groups

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

Console path:

Setup > **Firewall**

2.47.2.1 Name

Name of the group.

Console path:

Setup > **Firewall** > **Host-Groups**

Possible values:

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

2.47.2.2 Hostnames

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.

Console path:

Setup > **Firewall** > **Host-Groups**

Possible values:

Max. 255 characters from `comma separated list of IP addresses, networks or hostnames (with wildcards)`

2.47.3 Log-Actions

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.

Console path:

Setup > **Firewall**

Possible values:

No

Do not write an entry.

Yes

Write an entry.

2.59 WLAN-Management

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.

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.

If an access point is already being managed by a WLC, it will no longer try to contact the R&S®LANCOM Management Cloud.

This make it possible to use zero-touch commissioning, which means that no further configuration of the access point is necessary. In certain cases it may still be necessary to carry out a manual configuration. This can be done in the device configuration here.

Console path:

Setup

2.59.1 Static-WLC-Configuration

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.

Console path:

Setup > **WLAN-Management**

2.59.1.1 IP-Address

Set the IP address or DNS name of a WLAN controller.

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

Max. 44 characters from `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.59.1.2 Port

Configures the port used to attempt to reach a WLC.

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

0 … 65535

Default:

1027

2.59.2 Operating

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.

Console path:

Setup > **WLAN-Management**

Possible values:

No

The search for a WLC is disabled.

Yes

A WLC is actively searched for.

Default:

Yes

2.59.3 Update-Cert-Before

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

Console path:

Setup > **WLAN-Management**

Possible values:

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

Default:

30

2.59.4 Capwap-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. R&S®NC By default, WLCs also use this port.

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 65535

Default:

1027

2.60 Power

In this menu you will find settings for power management.

Console path:

Setup

2.60 Dual-PoE-Mode

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.

Console path:

Setup > **Power**

Possible values:

Hitless-Failover

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

For 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. Typically, the power drawn from both ports is similar, but this is ultimately influenced by the applied voltage and depends on the switch/PoE injector and/or cabling.

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

2.61 L2TP

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.

Console path:

Setup

2.61.1 Endpoints

The table contains the basic settings for the configuration of an L2TP tunnel.

To authenticate RAS connections by RADIUS and without configuring a router, this table needs a default entry with the following values:

- **Tunnel-Id**: DEFAULT
- **Auth-Peer**: Yes
- **Hide**: No

All other values must remain empty. With **Auth-Peer** set to “No” in the DEFAULT entry, all hosts will be accepted unchecked and only the PPP sessions are authenticated.

Console path:

Setup > **L2TP**

2.61.1.1 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.

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

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

2.61.1.2 IP-Address

The IP address of the tunnel endpoint. An FQDN can be specified instead of an IP address (IPv4 or IPv6).

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

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

2.61.1.3 Port

UDP port to be used.

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

0 … 65535

Default:

1701

2.61.1.4 Host name

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.

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

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

2.61.1.5 Password

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

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

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

2.61.1.6 Auth-Peer

Specifies whether the remote station should be authenticated.

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

Peer does not have to be authenticated.

Yes

Peer must be authenticated.

Default:

No

2.61.1.7 Hide

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

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

Tunnel negotiation is not obfuscated.

Yes

Tunnel negotiation is obfuscated.

Default:

No

2.61.1.8 Operating

This L2TP endpoint is enabled or disabled.

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

L2TP endpoint is disabled.

Yes

L2TP endpoint is enabled.

Default:

Yes

2.61.2 Ethernet

This table is used to link the L2TPv3 endpoints with a WLAN network.

Console path:

Setup > **L2TP**

2.61.2.1 L2TP-Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table (<xref href="2_61_1_1.dita"/>). This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need “to run” via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

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

2.61.2.2 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.

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

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

2.61.2.3 Interface name

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

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtual L2TP Ethernet interfaces

2.61.2.4 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.

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

68 … 1500

Default:

1500

2.62 LAN

This item contains the settings relating to the LAN connection of the access point.

Console path:

Setup

2.62.1 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.

Console path:

Setup > **LAN**

2.62.1.1 Name

This parameter shows the logical cluster interface used for bundling the selected physical interfaces of the devices.

Console path:

Setup > **LAN** > **LACP**

Possible values:

Max. 9 characters from `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

BUNDLE-0

2.62.1.2 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.

Console path:

Setup > **LAN** > **LACP**

Possible values:

No
Yes

2.62.1.3 Priority

Enter the LACP system priority.

Console path:

Setup > **LAN** > **LACP**

Possible values:

Multiples of 4096 `Max. 6 characters from [0-9]`

Default:

65535

2.62.1.4 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

Console path:

Setup > **LAN** > **LACP**

Possible values:

layer2
layer2+3
layer3+4
encap2+3
encap3+4

Default:

layer3+4

2.62.1.5 Ports

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

Console path:

Setup > **LAN** > **LACP**

Possible values:

Max. 16 characters from `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

ETH1,ETH2

2.62.2 Ethernet ports

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

Console path:

Setup > **LAN**

2.62.2.1 Port

Configure the Ethernet port that these settings apply to.

Console path:

Setup > **LAN** > **Ethernet-Ports**

Possible values:

Max. 10 characters from LAN port `ETHx|LANx`

2.62.2.2 Advertised-Rates

Configure the rates advertised for this Ethernet port here.

Console path:

Setup > **LAN** > **Ethernet-Ports**

Possible values:

Auto
100HDX
100FDX
1000FDX

Default:

Auto

2.62.2.3 Power-Saving

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

Console path:

Setup > **LAN** > **Ethernet-Ports**

Possible values:

No
Yes

2.62.3 Spanning-Tree

This menu contains the settings for the Spanning Tree Protocol.

Console path:

Setup > **LAN**

2.62.3.1 Operating

Here you can enable or disable support for Spanning Tree. When Spanning Tree is disabled, the router does not send Spanning Tree packets and forwards any received Spanning Tree packets instead of processing them itself.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

No
Yes

2.62.3.2 Port-Data

In this table, additional Spanning Tree parameters can be configured per port.

Console path:

Setup > **LAN** > **Spanning-Tree**

2.62.3.2.1 Port-Data

The name of the LAN interface.

Console path:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Possible values:

Max. 64 characters from LAN port `ETHx|LANx`

2.62.3.2.2 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 with the smaller number 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. Lower values yield higher priority.

Console path:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Possible values:

0
16
32
48
64
80
96
112
128
144
160
176
192
208
224
240

Default:

128

2.62.3.2.3 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.

Console path:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Possible values:

No
Yes

Default:

No

2.62.3.2.4 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.

Console path:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Possible values:

0 … 4294967295

Special values:

0

This value disables path cost influence.

2.62.3.3 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.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

0
4096
8192
12288
16384
20480
24576
28672
32768
36864
40960
45056
49152
53248
57344
61440

Default:

32768

2.62.3.4 Protocol-Version

The protocol can be selected here. Depending on the selection, either the Classic or Rapid protocol will be used, as defined in IEEE 802.1D-1998 chapter 8 or IEEE 802.1D-2004 chapter 17, respectively.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

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.

2.62.3.5 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”.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

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

Default:

15

2.62.3.6 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”.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

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

Default:

2

2.62.3.7 Max-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”.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

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

Default:

20

2.62.3.8 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.

Console path:

Setup > **LAN** > **Spanning-Tree**

Possible values:

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

Default:

6

2.70 IP-Configuration

Parameter for the IP configuration of the device.

Console path:

Setup

2.70.4 Static-Parameters

IP and network configuration 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 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.

Console path:

Setup > **IP-Configuration**

2.70.4.1 Interface-Name

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

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 64 characters from `INTRANET`

2.70.4.2 IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.70.4.3 IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.70.4.4 Primary-IPv4-DNS

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

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.70.4.5 Secondary-IPv4-DNS

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

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.70.4.6 Primary-IPv6-DNS

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

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.70.4.7 Secondary-IPv6-DNS

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

Console path:

Setup > **IP-Configuration** > **Static-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.70.6 LAN-Interfaces

Here you specify basic configuration options relating to your device's own IP settings and network access.

Console path:

Setup > **IP-Configuration**

2.70.6.1 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.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

Max. 64 characters from `INTRANET`

2.70.6.2 Interface-ID

The internal identifier for the interface. This cannot be modified.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

2.70.6.3 VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

0 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

2.70.6.4 IPv4-Address-Source

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

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

2.70.6.5 IPv6-Address-Source

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

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

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.

2.70.6.6 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.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

Max. 19 characters from `IPv4 address: a.b.c.d/xx`

2.70.6.7 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.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d/64`

2.70.6.9 Comment

Here you can enter a comment about the interface configuration.

Console path:

Setup > **IP-Configuration** > **LAN-Interfaces**

Possible values:

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

2.70.8 Untagged-VLAN

If a device has more than one Ethernet port, the other Ethernet ports can optionally be configured with an untagged VLAN. The untagged VLAN is used without a VLAN tag on the other LAN port and is used, for example, to integrate network devices that are not VLAN-capable. The other Ethernet port thus acts as an access port. The untagged ports and their VLAN tag are specified in this table.

Console path:

Setup > **IP-Configuration**

2.70.8.1 Port

Enter a port for the untagged VLAN.

Console path:

Setup > **IP-Configuration** > **Untagged-VLAN**

Possible values:

ETH1
ETH2
…

2.70.8.2 VLAN

Specify a VLAN ID for the untagged VLAN.

Console path:

Setup > **IP-Configuration** > **Untagged-VLAN**

Possible values:

0 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

2.99 LBS

R&S®NC access points are able to work 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.

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.

Console path:

Setup

2.99.1 HTTP-Server

Configure the HTTP endpoints for the LBS data here.

Console path:

Setup > **LBS**

2.99.1.1 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.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

Max. 251 characters from `URL with http or https`

2.99.1.3 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.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

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

2.99.1.4 Data-Sources

Here you configure the types of LBS data that should be sent. Only BLE is currently available.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

BLE

2.99.1.5 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.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

None
BLE-Address-Type-Transmit
BLE-Advertising-Data-Transmit
BLE-Name-Transmit
BLE-RSSI-Transmit
BLE-Scan-Response-Data-Transmit

2.99.1.6 Buffering-Timeout

After the configured time (in seconds) is reached, all BLE messages buffered up to that point are sent to the server.

With this value and *2.99.1.6 Buffer-Size* on page 165 both set to 0, the messages are sent to the server as soon as possible.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

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

Special values:

0

The value “0” means that no limitation is active.

2.99.1.6 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 this value and *2.99.1.6 Buffering-Timeout* on page 164 both set to 0, the messages are sent to the server as soon as possible.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

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

Special values:

0

The value “0” means that no limitation is active.

2.99.2 Operating

By turning on the BLE radio here, data about the BLE environment is collected continuously.

Console path:

Setup > **LBS**

Possible values:

No

BLE radio switched off.

Yes

BLE radio switched on.

Default:

No

2.99.3 LBS-Server-Type

Configure the LBS server type here. Currently, only the HTTP API with data packets in JSON format is supported.

Console path:

Setup > **LBS**

Possible values:

HTTP-JSON

2.99.4 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.

Console path:

Setup > **LBS**

Possible values:

Passive
Active

2.99.5 Run-Bluetooth-Scan

Use this action to run a Bluetooth scan.

Example: `do Run-Bluetooth-Scan`

Console path:

Setup > **LBS**

2.99.6 Delete-CA-Certificate

This action allows you to delete the certificate used for communication with an HTTPS server.

Example: `do Delete-CA-Certificate`

Console path:

Setup > **LBS**

2.99.7 Delete-Scan-Results

Use this action to delete the values of the last Bluetooth scan.

Example: `do Delete-Scan-Results`

Console path:

Setup > **LBS**

2.102 LMC

Settings for the configuration and monitoring of your device via the R&S®LANCOM Management Cloud (LMC).

Console path:

Setup

2.102.1 Operating

Specify whether the device should be managed via the LMC.

Console path:

Setup > **LMC**

Possible values:

No

The device does not connect to the LMC.

Yes

The LMC manages the device.

Default:

Yes

2.102.2 Proxy

If the connection from the device to the LMC is to be established via an HTTP proxy server, this can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

If the switch *2.102.2.4 Tunnel* on page 168 is also activated, a transparent tunnel is used via the proxy server using the HTTP CONNECT method. The proxy server must support this. If the switch is not activated, individual HTTP requests are forwarded via the proxy.

Console path:

Setup > **LMC**

2.102.2.1 URL

If the connection from the device to the LMC is to be established via an HTTP proxy server, this can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

Console path:

Setup > **LMC** > **Proxy**

Possible values:

Max. 256 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.102.2.2 Username

User name for use with an HTTP proxy server.

Console path:

Setup > **LMC** > **Proxy**

Possible values:

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

2.102.2.3 Password

Password for the user for use with an HTTP proxy server.

Console path:

Setup > **LMC** > **Proxy**

Possible values:

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

2.102.2.4 Tunnel

If a proxy URL has been specified and this switch is activated, a transparent tunnel is used via the proxy server using the HTTP CONNECT method. The proxy server must support this. If the switch is not activated, individual HTTP requests are forwarded via the proxy.

Console path:

Setup > **LMC** > **Proxy**

Possible values:

No
Yes

Default:

No

2.102.7 Delete-Certificate

Use this action to delete the LMC certificate.

Console path:

Setup > **LMC**

Possible arguments:

none

2.102.8 DHCP-Client-Auto-Renew

With this parameter you specify the behavior of the device in the event that there is a change to the DHCP settings in the network and the LMC client is unable to connect to the LMC.

If the LMC client is unable to reach its configured LMC, it is likely that the IP address range of the network has changed. A device that is configured as a DHCP client retains the IP address that was previously allocated to it until the DHCP lease time expires. By enabling this parameter, the device requests a new DHCP address (DHCP-Renew) regardless of the remaining DHCP lease time.

Console path:

Setup > **LMC**

Possible values:

No

If the LMC client loses its connection to the LMC, no DHCP-Renew is triggered.

Yes

If the LMC client loses its connection to the LMC, a DHCP-Renew is triggered. If the DHCP-Renew is not successful, the DHCP process is restarted. The device then tries to get an IP address from any DHCP server in order to reconnect to the LMC.

Default:

No

2.102.13 Configuration-Via-DHCP

Specify whether the LMC domain should be obtained from a DHCP server.

Console path:

Setup > **LMC**

Possible values:

No

The LMC domain is not obtained from a DHCP server. The value configured in the field **LMC-Domain** is taken.

Yes

The LMC domain is obtained from a DHCP server.

> In order for the DHCP server to provide the LMC domain, the DHCP server requires sub-option 18 of the DHCP option 43 to be set to the LMC domain. For further information about configuring the LMC parameters, see the LCOS Reference Manual section “Delivery of the LMC domain by the LCOS DHCP server”.

Default:

No

2.102.15 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.

Console path:

Setup > **LMC**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.16 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.

Console path:

Setup > **LMC**

Possible values:

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

2.102.17 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.

Console path:

Setup > **LMC**

Possible values:

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

2.102.18 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.

Console path:

Setup > **LMC**

Possible values:

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

2.102.200 Pairing-Token

Here you enter the activation code that you created for pairing with the LMC.

Console path:

Setup > **LMC**

Possible values:

Max. 36 characters from `^[1-9A-NP-Z-]{24,47}$|^$`

2.107 Automatic-Firmware-Update

The R&S®NC Auto Updater allows on-site R&S®NC devices to be updated automatically without further user intervention (unattended). 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.

Console path:

Setup

2.107.1 Mode

Set the operating mode of the R&S®NC Auto Updater.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

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.

check

The Auto Updater regularly checks the R&S®NC 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.

check-and-update

The Auto Updater regularly checks the R&S®NC update server for new updates. The update server uses the version 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.

Default:

check-and-update

2.107.2 Check-Firmware-Now

This command triggers the device to check the R&S®NC update server for new firmware.

Console path:

Setup > **Automatic-Firmware-Update**

2.107.3 Update-Firmware-Now

This command triggers the device to download and install the latest firmware from the R&S®NC update server.

Console path:

Setup > **Automatic-Firmware-Update**

2.107.4 Cancel-Current-Action

This command triggers the device to abort any current actions by the Auto Updater. This applies to manually started and scheduled actions.

Console path:

Setup > **Automatic-Firmware-Update**

2.107.5 Reset-Updater-Config

This command resets the boot-persistent configuration files that are created by the Auto Updater. This includes the local blacklist of firmware versions that failed an automatic update.

Console path:

Setup > **Automatic-Firmware-Update**

2.107.6 Base-URL

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

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default:

https://update.lancom-systems.de

2.107.7 Check-Interval

After booting, the Auto Updater sets a random time period within a day or a week for the check to be performed. The update itself is performed in the next time period between 02:00 - 04:00 (default).

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

daily
weekly

Default:

daily

2.107.8 Version-Policy

Set the version policy of the R&S®NC Auto Updater. This controls which firmware versions are offered to update a device.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

latest

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

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-updates-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-without-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.

Default:

security-updates-only

2.107.10 Check-Time-Begin

The hour of the day at the start of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, 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.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

2.107.11 Check-Time-End

The hour of the day at the end of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, 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.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

2.107.12 Install-Time-Begin

The hour of the day at the start of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

2

2.107.13 Install-Time-End

The hour of the day at the end of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

4

2.111 IoT

Settings for IoT technologies supported by LCOS LX, such as Wireless ePaper and Bluetooth Low Energy.

Console path:

Setup

2.111.1 USB

Configure the settings for USB Ethernet support here.

Console path:
Setup > **IoT**

2.111.1.1 CDC-EEM-Support

Configure the settings of the CDC-EEM protocol for USB Ethernet support here.

Console path:
Setup > **IoT** > **USB**

2.111.1.1.1 Operating

Switch USB Ethernet support on or off here.

Console path:
Setup > **IoT** > **USB** > **CDC-EEM-Support**

Possible values:

No
USB Ethernet support disabled.
Yes
USB Ethernet support enabled.

Default:

No

2.111.1.1.2 VLAN-ID

Optional specification of a VLAN ID.

Console path:
Setup > **IoT** > **USB** > **CDC-EEM-Support**

Possible values:
0 … 4095

2.111.88 Wireless ePaper

Configure the settings for the Wireless ePaper module here.

Console path:

Setup > **IoT**

2.111.88.1 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. The legacy connection mode via UDP is not supported by LCOS LX.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No

The Wireless ePaper feature is not enabled.

Yes

The Wireless ePaper feature is enabled.

Default:

No

2.111.88.2 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.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

2404 MHz
2410 MHz
2422 MHz
2425 MHz
2442 MHz
2450 MHz
2462 MHz
2470 MHz
2474 MHz
2477 MHz
2480 MHz

Default:

2404 MHz

2.111.88.3 Server-Address

IP address of the Wireless ePaper Server.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9].-:%`

2.111.88.4 Server port

The TCP destination port to be used for communication with the server.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

0 … 65535

Default:

7354

2.111.88.5 Protocol

The protocol used to communicate with the server.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

ThinAP2.0/TLS

Default:

ThinAP2.0/TLS

2.111.88.6 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.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No
Yes

Default:

No

2.111.88.7 Server-Hostname-Verification

In connection with the option *2.111.88.6 Server-Authentication* on page 179, 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.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No
Yes

Default:

No

2.111.88.10 Use-Separate-IP-Interface

This function lets you 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 different interface to the standard management IP/VLAN interface.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No

The separate IP interface for Wireless ePaper is not activated.

Yes

The separate IP interface for Wireless ePaper is activated. Configure these under *2.111.88.20 IP interface* on page 180 and *2.111.88.30 Static-IP-Parameters* on page 182.

Default:

No

2.111.88.20 IP interface

Configure the separate IP interface for connecting to the ePaper server or the Vusion Cloud.

Console path:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.20.1 Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 64 characters from `INTRANET|Wireless-ePaper`

Default:

Wireless-ePaper

2.111.88.20.2 Interface-ID

The internal identifier for the interface. This cannot be modified.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 16 characters from `br-lan|epaper`

Default:

ePaper

2.111.88.20.3 VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

2 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

2.111.88.20.4 IPv4-Address-Source

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

2.111.88.20.5 IPv6-Address-Source

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

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.

2.111.88.20.6 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.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 19 characters from `IPv4 address: a.b.c.d/xx`

2.111.88.20.7 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.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d/64`

2.111.88.30 Static-IP-Parameters

Here you configure the IP and network settings that apply when you use static IP addresses.

Console path:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.30.1 Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 64 characters from `INTRANET|Wireless-ePaper`

Default:

Wireless-ePaper

2.111.88.30.2 IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.111.88.30.3 IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.111.88.30.4 Primary-IPv4-DNS

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.111.88.30.5 Secondary-IPv4-DNS

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

2.111.88.30.6 Primary-IPv6-DNS

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.111.88.30.7 Secondary-IPv6-DNS

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

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

3 Firmware

This menu contains the actions and settings options for managing the device firmware.

Console path:

/

3.2 Table-Firmsafe

For each of the two firmware versions stored in the device, this table contains information on the memory space number (1 or 2), and the status (active or inactive).

Console path:

Firmware

3.2.1 Position

Position in memory space of the current entry.

Console path:

Firmware > **Table-Firmsafe**

3.2.2 Status

Status of the current entry.

Console path:

Firmware > **Table-Firmsafe**

Possible values:

active

This firmware is currently in use in the device.

inactive

This firmware is in a wait state and can be activated.

3.8 Switch firmware

This command line is used to switch the active firmware into the inactive state. Correspondingly, the alternative, non-active firmware is switched to the active state.

The device restarts automatically and immediately starts using the alternative firmware. By switching again, you restore the initial state.

Console path:

Firmware

Possible values:

`do Switch-Firmware`

Switch the firmware and restart the device

3.10 Boot-count

Saves the number of restarts performed by the device with the current firmware.

Console path:

Firmware

4 Other

This menu contains additional functions from the LCOS LX menu tree.

Console path:
/

4.1 Reset-Config

This action allows you to reset the configuration.

Example: `do Reset-Config`

Console path:
Other

4.2 Reboot

This action is used to restart the device.

Example: `do Reboot`

Console path:
Other

4.3 Delayed-Reboot

This action is used to restart the device after a delay. The delay is specified in seconds.

Example: `do Delayed-Reboot 30`

Console path:
Other

4.3 Cancel-Delayed-Reboot

This action lets you interrupt a delayed restart initiated with `do Delayed reboot` within the delay time.

Example: `do Cancel-Delayed-Reboot`

Console path:

Other

4.5 Delete-Support-Info

Use this action to delete the persistent boot log and core dumps created after a crash.

Example: `do Delete-Support-Info`

Console path:

Other

1 Status

This menu provides status information.

Console path:

/

1.62 Syslog

This menu provides status information about Syslog.

Console path:

Status

1.62.1 Last-Messages

This table displays the Syslog messages. Example:

```
Id Time           Priority  Message                                                LMC-Message-ID
===-------------------------------------------------------------------------------------------------
0  1786102398625  err       "lxcron[6204]: Service temporarily not available"  5c9f6e94-e39a-...
1  1786102399918  notice    "mcastds: Entering evloopRun"                      4276b3ac-bfc9-...
2  1786102403656  err       "lxcron[7226]: Service temporarily not available"  38b0a6cc-e95b-...
```

Console path:

Status > **Syslog**

1.62.1.1 Id

ID of a Syslog message.

Console path:

Status > **Syslog** > **Last-Messages**

Possible values:

max. 5 Zeichen aus `[0-9]`

1.62.1.2 Time

Timestamp of a Syslog message.

Console path:

Status > **Syslog** > **Last-Messages**

Possible values:

max. 20 Zeichen aus `[0-9]`

1.62.1.3 Priority

Severity level of a Syslog message.

Console path:

Status > **Syslog** > **Last-Messages**

Possible values:

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

1.62.1.4 Message

Message text of a Syslog message.

Console path:

Status > **Syslog** > **Last-Messages**

Possible values:

max. 255 Zeichen aus `[A-Z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

1.62.1.5 LMC-Message-ID

LMC message ID of a Syslog message.

Console path:

Status > **Syslog** > **Last-Messages**

Possible values:

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