LCOS 10.90

Menu Reference

04/2025

LANCOM SYSTEMS

Contents

Copyright

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Introduction

1.1 About this documentation

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, WEBconfig or via the serial interface?
- How is the device assigned to the 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, the operating system used by the devices. This guide is an aid to users during the configuration of devices by means of WEBconfig or the CLI. The parameters are listed in the alphabetical order of the paths as they appear in SNMP. 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.eu/download*.

LCOS, the operating system of the LANCOM devices

All routers, gateways, controllers and access points from LANCOM Systems work with the same operating system: LCOS. A proprietary development of LANCOM, this operating system is highly resistant to external attack and provides a high level of security.

The consistent use of LCOS also ensures that operation is easy and uniform between products. The extensive feature set with all products is immediately available. Free, regular software updates are constantly under development.

Validity

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

This documentation was created by…

…members of our staff from a variety of departments in order to ensure you the best possible support when using your product. If you should find any mistakes, have a criticism, or wish to suggest any improvements, please do not hesitate to contact us.

E-mail: info@lancom-systems.de

If you have any questions on the content in this manual, or if you require any further support, our Internet server www.lancom-systems.com is available to you around the clock. The 'Support' section will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledge base offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download. You can also refer to LANCOM support. For telephone numbers and contact addresses for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Web site.

1.2 Configuration with Telnet

Open Telnet session

To commence the configuration, start Telnet from the Windows command line with command:

```
C:\>telnet 10.0.0.1
```

Telnet establishes a connection to the device with the IP address entered.

After entering the password (assuming one has been set to protect the configuration) all of the configuration commands are available to you.

Linux and Unix additionally support Telnet sessions via SSL-encrypted connections. Depending on the distribution it may be necessary to replace the standard Telnet application with an SSL-capable version. Start the encrypted Telnet connection with the following command:

```
C:\>telnet -z ssl 10.0.0.1 telnets
```

Changing the console language

Terminal mode is available in English or German. The devices are set with English as the standard console language. . If necessary, change the console language with the following commands:

WEBconfig: /Setup/Config-Module/Language

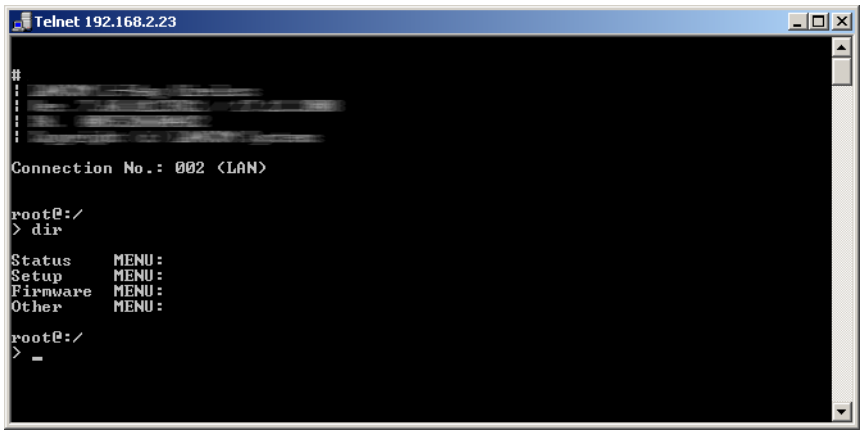
Close the Telnet session

To close the Telnet session, enter the command `exit` at the command prompt:

```
C:\>exit
```

Structure of the command-line interface

The LCOS command-line interface is structured as follows:



Status

Contains the states and statistics of all internal modules in the device and the direct access to the file system

Setup

Contains all adjustable parameters of all internal modules in the device

Firmware

Contains the firmware management

Other

Contains actions for establishing and terminating connections, reset, reboot and upload

1.3 Commands for the CLI

The LCOS command-line interface is operated with the following commands. Some of the available menu commands can be displayed using the HELP command.

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

Some commands require special privileges in order to run, and these are listed along with the respective command. Commands that do not specify any rights have no restrictions.

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

Command	Description
`add|set [<Path>] <Value(s)>`	Sets a configuration parameter to a particular value. If the configuration parameter is a table value, a value must be specified for each column. Entering the * character leaves any existing table entry unchanged. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`add|set [<Path>] ?`	Lists all possible input values for a configuration parameter. If no specific path is entered, the possible input values for all configuration parameters in the current directory are listed. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write

Command	Description
`beginscript [-u] [-C d] [-s <password>]`	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. Possible arguments are: › `-u`: Forces the **u**nconditional execution of a script or a configuration. › `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used. › `-s`: Decrypts the script with the password used for `readscript -s`. **Access rights**: Supervisor-Write
`bootconfig [-s (1|2|all)] [-r (1|2|all)]`	Enables you to save and delete boot configurations. Options: › `-s`: Stores the current configuration of a device either as a custom default setting (1), rollout configuration (2), or both (all). › `-r`: Optionally deletes the current custom default setting (1), the rollout configuration (2), or both (all). **Access rights**: Supervisor-Write
`cd <Path>`	Switch to the current directory. Various abbreviations can be used, such as replacing `cd ../..` with `cd ...`, etc.
`clear`	Clears the current CLI output. All previously entered commands can be viewed by means of the log.
`default [-r] [<Path>]`	Resets individual parameters, tables or entire menu trees back to their default configuration. If `<PATH>` indicates a branch of the menu tree, then the option `-r` (recursive) must be entered. **Access rights**: Supervisor-Write
`del|delete|rm [<Path>] <Row>|*`	Deletes the table row `<Row>` in the current table or the table referenced in the branch of the menu tree with `<Path>`. Enter the line number for the `<Row>`. The wildcard symbol `*` deletes a table, for example, `del Config/Cron-Table *`. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`deletebootlog`	Clears the contents of the persistent boot log memory.
`dir|list|ls|llong|l [-a] [-r] [-s] [<Path>] [<Filter>]`	Displays the current directory content. Possible arguments are: › `-a`: In addition to the content of the query, this also lists the SNMP IDs. The output begins with the SNMP ID of the device followed by the SNMP ID of the current menu. The SNMP IDs of the subordinate items can be read from the individual entries. › `-r`: Also lists all subdirectories as well as the tables they contain. › `-s`: Sorts the display of the current directory; grouped by sub directories, tables, values, and actions; in ascending alphabetical order.
`dnsquery [-t <type>] [-d <destination>] name[@rtg-tag]`	Resolves DNS requests. Possible parameters: › `name`: The DNS name to resolve. › `@rtg-tag`: Optional routing tag for reaching the DNS server. › `-t <type>`: Type: A, AAAA, PTR, SRV, NAPTR › `-d <destination>`: Destination used for reaching the DNS servers. As in the forwarding table, a routing tag can also be specified if the forwarding destination is an IP address (e.g. 8.8.8.8@4095). You can also specify two

Command	Description

	comma-separated IP addresses (with an optional routing tag) (e.g. 8.8.4.4@4095,8.8.8.8@4095). The DNS client switches between servers if one does not respond
	
	If the command is entered without options, i.e. with the mandatory domain name only, then a request of type AAAA as well as a request of type A will be issued. Example:
	`> dnsquery www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	The AAAA-type response is only issued if the IPv6 address can also be reached.
	
	The type can also be specified explicitly using the option `-t`. The available types are AAAA, A, PTR, SRV and NAPTR. In the case of a PTR request, the requested IP address must be specified directly and may not be converted in the "ARPA" string:
	`> dnsquery -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	
	Because the dnsquery command uses the DNS client of the LANCOM device, its behavior is determined by the DNS configuration of the device (i.e. forwarding, loopback addresses, etc.). Since the DNS configuration may differ depending on the routing tag, the dnsquery command can be used to append the requested name (or to the requested address in the case of PTR requests) by means of an @ extension:
	`> dnsquery www.lancom.de@4095`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	It is also possible to send the requests while bypassing the forwarding configuration by specifying the -d parameter. Anything that can be specified as a destination in the forwarding table can also be specified as a destination here. With the destination set manually, the loopback address is set according to the loopback configuration. Example: AAAA+A request via WAN connection INTERNET
	`> dnsquery -dinternet www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	To do this, a DNS server must of course have been assigned to the INTERNET WAN connection, e.g. via PPP, DHCP, or manually in the IP parameter list.
	
	Example: PTR request via Google server
	`> dnsquery -d8.8.8.8 -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	
	If no server responds, the client retries three times at increasing intervals, i.e. after each request, it waits 1, 2, 4, and finally 8 seconds. If there is no answer by then, the request is canceled. Pressing <CR> while a request is ongoing causes it to be canceled.

`do <Path> [<Parameter>]`	Executes the action in the current or the referenced directory, for example, do `Other/Coldstart`. If the action has additional parameters, they can be added at the end.

Command	Description
`echo <Argument>`	Displays the commands on the CLI.
`enable <Parameter>`	Extends the rights of authenticated TACACS+ users. Possible parameters are: › `0`: No rights › `1`: Read-only › `3`: Read-write › `5`: Read-only-limited Admin › `7`: Read-write-limited Admin › `9`: Read-only Admin › `11`: Read-write Admin › `15`: Supervisor (root)
`ethping -i <interface> [-?] [-c count] [-v vlan] [-s size] [-l mdlevel] <target address>`	CFM Ethernet Ping.
`exit|quit|x`	Ends the terminal session.
`feature <Code>`	Activates the software option with the specified activation code. **Access rights**: Supervisor-Write **Command line options:** **Feature <activation-code>** Activation using activation code **Feature -Q** Query status of current and past remote activation requests **Feature -q** <query-id> Query status of a single request Feature -l <license-key> -t <license-type> [-i <license-index>] [-a <source-address>] [-u <server-url>] [-c <contact-data>] start a new remote activation request. Progress can be tracked using -q/-Q **-a <source-address>** source IP address or interface, e.g. INT, DMZ, LBx **-l <license-key>** 16/19 character license key **-t <license-type>** type of license, e.g. VPN25 **-i <license-index>** index of existing license for extension, 0 for additional license **-u <server-url>** URL of the license server **-c <contact-data>** comma separated list of contact details
`find <term>`	Looks for the search <term> and outputs all menu items containing it.
`flash yes|no`	Regulates the storing of configuration changes using the command line. By default, changes to the configuration using commands in the command line are written directly to the boot-resistant Flash memory of the devices (`yes`). If updating the configuration is suppressed in the Flash memory (`no`), changes are only stored in RAM (deleted on booting). **Access rights**: Supervisor-Write
`getenv <Name>`	Lists the respective environmental variables (without line feed). Please also note the command "printenv".

Command	Description
`history`	Displays a list of recently executed commands. Command `!#` can be used to directly call the list commands using their number (#): For example, `!3` executes the third command in the list.
`ikectl [-[r|d|D] <peer-name-list>] [-[e|r|d] <ipsec-name-list>] [-[r|d] [<ike-cookies-list>|<esp-spi-list>]] [-R <peer-name-list> <redirect-target>]`	This command widens the range of analysis options, for example by executing targeted actions to isolate the problem in the event of an error. This function allows you to quickly and automatically modify and test a VPN, among other things. › `-e <ipsec-name-list>`: Creates a Phase 2-SA/CHILD_SA when entered with the VPN rule name › `-r <peer-name-list>`: Performs a rekeying of the Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer › `-r <ike-cookies-list>`: Performs rekeying when entered with the IKE cookie › `-r <ipsec-name-list>`: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the name of the VPN rule › `-r <esp-spi-list>`: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI › `-d <peer-name-list>`: Deletes a Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer › `-d <ike-cookies-list>`: Deletes a Phase 1-SA / IKE_SA when entered with IKEv1 cookies / IKEv2 SPIs › `-d <ipsec-name-list>`: Deletes a Phase 2-SA/CHILD_SA when entered with the VPN rule name › `-d <esp-spi-list>`: Deletes a Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI › `-D <peer-name-list>`: Starts the liveness check (Dead Peer Detection – DPD) when entered with the name of the VPN remote peer › `-R <peer-name-list> <redirect-target`: Redirects IKEv2 remote sites to a new destination using the IKEv2 redirect. If the list of remote sites is empty, all remote sites are redirected. This command can be used for maintenance purposes to move VPN remote sites from the current VPN gateway to another gateway securely. › `<peer-name-list>`: List of remote peer names separated by spaces and consisting of max. 16 characters › `<ipsec-name-list>`: Space-separated list of VPN rule names, as displayed in “show vpn” as ipsec-0-PEER-pr0-l0-r0. ⓘ To find a certain CHILD_SA/Phase 2-SA for a road warrior, it is important to also specify the remote station name as follows: `"peer-name ipsec-name"`. › `<ike-cookies-list>`: Consists of a list of 16 hexadecimal values separated by spaces, e.g 0x000102030405060708090A0B0C0D0E0F › `<esp-spi-list>`: Consists of a list of 4 hexadecimal values separated by spaces, e.g. 0x00010203 › `<redirect-target>`: Target to which the remote site(s) are to be redirected. The target can be an IPv4 address, IPv6 address or a DNS name Example: `ikectl -r peer ipsec-name-peer-2 -D peer3 -d peer4 0x12345678 -e "RoadWarrior IPSEC-0-DEFAULT-PR0-L0-R0"`

Command	Description
`importfile -a <application> [-p <passphrase>] [-n] [-h <Hash> -f <Fingerprint>] [-c] [-r]`	Your device supports the loading of files into file slots from the console and also by means of a script. This offers the convenience of using a script to roll-out files together with the configuration or, for example, to import SSH keys and VPN certificates. **Required parameters:** **-a <application>** <application> specifies the storage location and thus the usage for the entered data. For a complete list of the storage locations on your device, enter importfile -?. **Optional parameters:** **-n** -n starts the non-interactive mode. There are no prompts or other outputs on the CLI. The non-interactive mode is intended for use with scripts. **-p <passphrase>** <passphrase> is the password required to decrypt an entered private key. **-h <hash>** The hash algorithm used to determine the fingerprint of the root CA certificate. **-f <fingerprint>** The fingerprint of the root CA certificate, created with –h. The fingerprint can be entered either with or without colons. **-c** Only CA certificates are uploaded. **-r** Uploaded CA certificates replace any existing ones.
`iperf [-s|-c <Host>] [options]`	Starts iPerf on the device to perform a bandwidth measurement with an iPerf2 counterpart. Possible options include: › **Client/Server** › `-u, --udp`: Uses UDP instead of TCP. › `-p, --port <Port>`: Connects to or expects data packets on this port (default: 5001). › `-q, --quiet`: Activates the quiet mode, suppressing CLI output since the command can also be invoked via the action table. Also prevents interruption of the execution in client mode. › **Server-specific** › `-s, --server`: Starts iPerf in server mode and waits for a connection from an iPerf client. › **Client-specific** › `-c, --client <Host>`: Starts iPerf in client mode and connects to the iPerf server <Host> (IP address or DNS name). › `-b, --bandwidth [<Bandwidth>/]<Bandwidth>{kKmM}`: Limits bandwidth for analyzing a UDP connection in the [Down-]/Up-Stream. The value is specified in kilobytes (kK) or megabytes (mM) per second (default: 1 Mbps). › `-l, --len <Length>`: Specifies the length of UDP data packets.

Command	Description
	› `-t, --time <Time>`: Specifies the duration of the connection in seconds (default: 10 seconds). › `-d, --dualtest`: Conducts a bidirectional test: iPerf server and client simultaneously send and receive. › `-r, --tradeoff`: Conducts a sequential test: iPerf server and client alternately send and receive. › `-R, --reverse`: Reverses the measurement direction. › `-L, --listenport <Port>`: Specifies the port on which the device expects data packets from the remote iPerf server in bidirectional mode (default: 5001). › `-P, --parallel <Number>`: Specifies the number of parallel client tasks (maximum: 20). › `-B, --bind <Interface>`: Restricts the connection to the specified interface (IP address or interface name). › `-E, --peer <Interface>`: Establishes a connection using the interface specified by the peer name and sets rx/tx thresholds based on the result(s). If not executed in dual or tradeoff mode, the value of the unmeasured direction is set based on the last measurement if available. The result is recorded in the status table **Status** > **Iperf** > **Last-Results** > **Peer-Result** (1.96.1.3) under the values **Peer**, **Server-Bandwidth-kbps**, and **Client-Bandwidth-kbps**. › `--retry #`: Number of retry attempts if a connection cannot be established. Maximum: 99. › `--force`: If another client instance is already running, the system will wait until it is finished before proceeding. › `--ratediffperc #`: Maximum permitted rate deviation in percent in peer mode. Maximum: 99. › `--expbandwidth #/#{kKmM}`: Expected down/up stream bandwidth in peer mode. Values for unmeasured directions are ignored. Example: 10/10M › `--minbandwidth #{kKmM}`: Sets the specified value if the measurement returned a lower result. › **Miscellaneous** › `-h, --help`: Displays the help text.
`killscript <Name>`	Deletes the remaining unprocessed content of a script session Select the script session using its name. **Access rights**: Supervisor-Write
`language`	Selects a language for the CLI display. The command `language ?` lists the available languages.
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) is a command-line tool specified in RFC 6835 to query LISP mappings on a map resolver. Possible arguments are: › `-i <instance>`: Name of the LISP instance used for the destination query › `-m <server>`: LISP map server used for the destination query › `-id <num>`: LISP Instance ID [0-16777215] used for the destination query › `destination-eid`: Requested destination EID › `-retries <num>`: LISP retries to the map server [0-10]

Command	Description
	› `-rtg-tag <num>`: Routing tag used › `-source-eid <num>`: Source EID used Example: `lig -i LISP-INST 172.16.200.1`
`linktest`	Only available on WLAN devices. It displays the results of the WLAN link test. **Access rights**: Supervisor-Write **Execution right**: WLAN link test
`ll2mdetect`	Searches for devices via LL2M in the LAN. **Access rights**: Supervisor-Write
`ll2mexec`	Sends one command per LL2M to a device in the LAN. **Access rights**: Supervisor-Write
`loadconfig (-s <server IP address> -f <filename>)|<URL>`	Uploads a configuration file to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. The cron table works with the user configured for it, meaning that if "loadconfig" is executed via the cron table, it will only be able to read the configuration completely if it is run with the root administrator. **Access rights**: Supervisor-Write

`loadfile [-a <Address>] [-s <Server-IP-address>] [-n] [-f <File-name>] [-o <File-name>] [-c <File-name>] [-p <File-name>] [-d <Passphrase>] [-C n|d] [-m <Version>] [-u] [-x <File-name>] [-i]`	Uploads a certificate file to the device. Possible arguments are:
	› `-a`: Specifies the source address of the file:
	  › `a.b.c.d`: Source IP address
	  › `INT`: Use the address of the first intranet interface as the source address
	  › `DMZ`: Use the address of the first DMZ interface as the source address
	  › `LBx`: Use the loopback address x (0..f) as the source address
	  › `<Interface>`: Use the address of the LAN interface <interface> as the source address
	› `-s`: Address of the TFTP server
	› `-n`: Ignore server name on SSL/TLS connections
	› `-f`: <File name> of the configuration file on the TFTP server
	› `-o`: Destination file <file name>for file download
	› `-c`: File <file name> with the root certificate for HTTPS
	› `-p`: File <file name> with unencrypted PKCS#12 container for HTTPS CA certificates and / or client-side authentication
	› `-d`: <Passphrase> to decrypt downloaded encrypted PKCS#12 containers
	› `-C`: Checks whether firmware is newer than (n) or different from (d) the current firmware
	› `-m`: Set a minimum <version> of the firmware
	› `-u`: Download firmware file unconditionally; skip the version check.
	› `-x`: File <file name> with additional CA certificates for HTTPS checks; the value ' none' prevents the default certificates from being downloaded
	› `-i`: Send Sysinfo as a POST request (for HTTP(S) only)

Command	Description
	The options [-f] and [-s] and the URL cannot be used simultaneously. For HTTP(S) downloads, you must specify the source by means of a URL. The maximum length of the URL is 252 characters. **Access rights**: Supervisor-Write
`loadfirmware [-e] (-s <server IP address> -f <filename>)|<URL>`	Uploads firmware to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. The `-e` option switch causes the firmware file to be saved completely in the local file system first before the firmware update starts. **Access rights**: Supervisor-Write
`loadscript (-s <server IP address> -f <filename>)|<URL>`	Uploads a configuration script to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. The cron table works with the user configured for it, meaning that if "loadscript" is executed via the cron table, it will only be able to read the configuration completely if it is run with the root administrator. **Access rights**: Supervisor-Write
`lspci`	Output of information via PCI devices **Access rights**: Supervisor-Read
`ping <IPv4-Address|Hostname>` `ping -6 <IPv6-Address>%<Scope>`	Sends an ICMP echo request to the IP address specified. For more information about the command and the specifics of pinging IPv6 addresses, see the section *Parameter overview for the ping command* on page 39.
`printenv`	Shows an overview of all environmental variables and their values.
`readconfig [-h] [-s <password>]`	Shows the complete configuration in the format of the device syntax. › `-h`: Adds a checksum to the configuration file. › `-s <password>`: Encrypts the configuration file with the use of the specified password. **Access rights**: Supervisor-Read
`readmib`	Display of the SNMP Management Information Base. Available only on devices without a unified MIB. **Access rights**: Supervisor-Read,Local-Admin-Read
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	The readscript command generates a text dump of all commands and parameters required to configure the device in its current state. You can use the following option switches for this: › `-n`: The text output is only numerical without identifiers. The output only contains the current status values of the configuration as well as the associated SNMP IDs. › `-d`: The default values are included in the text output. › `-i`: The table designations are included in the text output. › `-c`: Includes any comments contained in the script file. › `-m`: The text is output to the screen in a compact but difficult to read format (no indentations). › `-h`: Adds a checksum to the script file. › `-s <password>`: Encrypts the script file with the use of the specified password. › `-o`: Replaces the passwords with a "*" to obfuscate them in the text output.

Command	Description
	Access rights: Supervisor-Read
`readstatus`	Outputs the status of all SNMP IDs for the device.
`release [-x] *|<Interface_1…Interface_n>`	The DHCPv6 client returns its IPv6 address and / or its prefix to the DHCPv6 server. It then submits a new request for an address or prefix to the DHCPv6 server. Depending on the provider, the server assigns a new address to the client, or reassigns the previous one. Whether the client receives a different address or prefix is determined solely by the server. The option switch `-x` suppresses the confirmation message. The `*` wildcard applies the command on all of the interfaces and prefix delegations. Alternatively, you can specify one or more specific interfaces.
`repeat <Interval> <Command>`	IPv6 address release: Repeats the specified command every `<Interval>` seconds until the process is ended with new input.
`rollout (-r|-remove) <RelatedFile>`	Deletes the files of the user-specific rollout wizard from the file system of the device. Possible files are: › `wizard`: Deletes the wizard › `template`: Deletes the template › `logo`: Deletes the logo › `all`: Deletes the wizard, the template and the logo
	Access rights: Supervisor-Write
`setenv <Name> <Value>`	Sets an environmental variable to the specified value.
	Access rights: Supervisor-Write, Local-Admin-Write, Limited-Admin-Write
`setpass|passwd [-u <User>][-n <new> <old>]`	Changes the password of the current user account. In order to change the password without a subsequent input prompt, use the option switch `-n` while entering the new and old password. The password can have a maximum of **128 characters** and use the following characeter set: #<>@ABDEFGHIJKMNOPQRSTUWXYZ{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuwxyz ` If the command `passwd` is deployed in a script and a `$` is used in the password, an additional `$` has to be prepended, as it would otherwise be interpreted as a variable and setting the password would fail. In order to change the password of the local user account when authentication by TACACS+ is enabled, use the option switch `-u` with the name of the corresponding user. If the local user does not exist or the user name is missing, the command aborts. The user must also have supervisor rights, or authorization by TACACS must be enabled.
`show <Options> <Filter>`	Shows selected internal data, such as › `admin-distance` – shows the administrative (routing) distance of all internal applications or routing protocols › `bootlog` – the last boot processes › `filter` – firewall filtering rules › `Fw-dns-destinations` – Optionally accepts a space-separated list of names of the firewall's DNS destinations. All DNS destinations or the ones

Command	Description
	specified in the parameter are listed sequentially. For each destination, the counter from **Status** > **Firewall** > **DNS-Database** > **Destination-Usage** is displayed, followed by the list of wildcard expressions. For each wildcard expression, the currently resolved addresses and the data records that are a direct or indirect match are displayed. › `ip-addresses` – displays all IPv4 and IPv6 addresses for the device for the LAN and WAN interfaces, along with advanced status information › `ipv4-addresses` – displays all IPv4 addresses for the device for the LAN and WAN interfaces, along with advanced status information › `lisp instance` – displays status information about all configured LISP instances › `lisp instance [instance]` – displays status information about the LISP instance named [instance] › `lisp map-cache` – displays status information about the map cache entries available for all instances › `lisp map-cache [instance]` – displays status information about the map cache entries for the instance named [instance] › `lisp registrations` – displays status information about the EIDs/RLOCs of all instances registered with the map server › `lisp registrations [instance]` – displays status information about the EIDs/RLOCs of the instance named [instance] registered with the map server › `lta` – shows information about groups or users of the LANCOM Trusted Access. This is set up and managed via the LANCOM Management Cloud. › `mem`, `heap` – memory usage › `netflow collectors` – displays information about the configured NetfFlow collectors › `netflow interfaces` – displays information about interfaces and the corresponding NetFlow parameters › `netflow metering-profiles` – displays information about the metering profiles of NetFlow/IPFIX › `VLAN` – dynamically added VLANs and VLAN memberships, e.g. added to the static configuration at runtime by CAPWAP or WLAN/802.1X › `VPN` – VPN rules With additional filter arguments you can further limit the output. For an overview of all possible options, enter `show ?`. The filters available with an option are displayed by `show <option> ?`. For example, `show VPN ?` shows the filters available for the VPN rules. For information on displaying IPv6-specific data, read the section *Overview of IPv6-specific show commands* on page 45. **Access rights**: Supervisor-Read, Local-Admin-Read
`sleep [-u] <Value><Suffix>`	Delays the processing of configuration commands by a particular time or terminates them at a particular time. Applicable values for `<SUFFIX>` are `s`, `m` and `h` for seconds, minutes and hours. If no suffix is defined, the command uses milliseconds. With option switch `-u`, the `sleep` command accepts times in format `MM/DD/YYYY hh:mm:ss` (English)

Command	Description
	or in format `TT.MM.JJJJ hh:mm:ss` (German). Times will only be accepted if the system time has been set.
`smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)`	Available only on devices with 3G/4G WWAN module: Sends a text message to the destination number entered. › `-s <SMSC-Number>`: Alternative SMSC phone number (optional). If you omit this part of the command, the device uses the phone number stored on the USIM card or that configured under SNMP ID 2.83. › `-d <Destination>`: Destination phone number › `-t <Text>`: Contents of the message with <=160 characters. For an overview of available characters, see the section *Character set for sending SMS* on page 51. Special characters must be in UTF8 encoded form.
`ssh [-?|h] [-o "option=value"] [-<a|b> Loopback-Address] [-p Port] [-C] [-j Keepalive-Interval] <Host>`	Establishes an SSH connection to the <Host>. Possible arguments are: › `-?|h`: Outputs the help text. › `-o "option=value"`: additional options with corresponding values can be specified. › `-a|b`: Allows a route or loopback address to be specified for the device to use if the destination can be reached via multiple routes. The function of `-a` and `-b` is identical. `-b` is the usual option used by an OpenSSH client on UNIX systems, whereas some other commands integrated into LCOS use `-a` to specify a loopback address. › `-p`: Sets the <Port> of the host › `-C`: Enforces compressed data transfer › `-j`: Specifies how frequently the client sends a keepalive.
`sshcopyid`	To store your SSH public key using SSH **Access rights**: Supervisor-Write

`sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <file-name>] [-R <host-name>]`	Creates or deletes the SSH key in the device. Possible arguments are:
	› `-h`: Displays a brief help text about the available parameters
	› `-q`: The device overrides existing keys without a prompt (quiet mode)
	› `-t`: This parameter specifies what type of key is generated. SSH supports the following types of keys:
	  › RSA
	  › DSA
	  › ECDSA
	  › ED25519
	  › ED448
	› `-b`: This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.
	› `-f`: These parameters specify the file name of the generated key file in the device file system. The choice of the file name depends on the type key you are generating. The choices available to you are:
	  › **ssh_rsakey** for RSA keys
	  › **ssh_dsakey** for DSA keys
	  › **ssh_ecdsakey** for ECDSA keys
	  › **ssl_privkey** for SSL-RSA keys
	  › **ssh_ed25519key** for Ed25519 keys

Command	Description
	› **ssh_ed448key** for Ed448 keys › `-R`: Removes all keys for a specific hostname. Optionally, specify a key type.
`ssldefaults [-y]`	This command resets the SSL / TLS settings in all submenus of the current configuration to the default values after a security prompt. In LCOS, each module comes with its own submenu for SSL / TLS settings. This provides a way to reset all settings in these various submenus to the current secure default settings. The parameter `-y` ensures that the security prompt is automatically answered so that the command can be used non-interactively in scripts.
`stop`	Ends the ping command
`sysinfo`	Shows the system information (e.g., hardware release, software version, MAC address, serial number, etc.).
`tab`	For use in script files: For the command that follows, this sets the order of the columns for the arguments in the case that the columns in the table differ from the default (e.g. a column was added). **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`telnet <Address>`	Establishes a Telnet connection to the given <address>.
`testmail <From> <To_1…To_n> [<Realname> <Subject> <Body>]`	Sends a test e-mail. A sender address and receiver address are necessary; real name, subject line and message content are optional. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`time <DateTime>`	Sets a time in format `MM/DD/YYYY hh:mm:ss`. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write **Execution right**: Time Wizard
`trace <Parameter> <Filter>`	Starts a trace command for output of diagnosis data. With additional filter arguments you can further limit the output. For further information on this command refer to the section *Parameter overview for the trace command* on page 41. **Access rights**: Supervisor-Read,Limited-Admin-Read,Limited-Admin-Write
`unmount [-?][-f] <Volume>`	Outputs the current volume table. › `-f`: Releases the specified volume. <Volume> may be the volume ID or any mount point. › `-?`: Outputs the help text.
`unsetenv <Name>`	Deletes the specified environmental variable. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`wakeup [MAC]`	Performs a Wake On LAN for the device with the MAC address [MAC]. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`who`	Lists active configuration sessions.
`writeconfig [-u] [-C d] [-s password] [-b index]`	Writes a new configuration on the device in the syntax format for the device. The system interprets all of the following lines as configuration values until two empty lines are read. Possible arguments are: › `-u`: Forces the **u**nconditional execution of a script or a configuration. › `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used. › `-s password`: Decrypts the configuration file with the use of the specified password.

Command	Description
	› `-b index`: Writes the configuration as an alternative boot configuration. Index must be `1`, `2` or `all`. **Access rights**: Supervisor-Write
`writeflash`	Load a new firmware file (only via TFTP). **Access rights**: Supervisor-Write
`!!`	Repeat last command
`!<num>`	Repeat command <num> times
`!<prefix>`	Repeat last command beginning with <prefix>
`#<blank>`	Comment

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 "/" or "\".
  - `..` 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 `sysinfo` can be shortened to `sys` and `cd Management` to `c ma`. The input `cd /s` is not valid, however, since it corresponds to both `cd /Setup` and `cd /Status`.
- Directories can be addressed with the corresponding SNMP ID. For example, the command `cd /2/8/10/2` has the same effect as `cd /Setup/IP-router/Firewall/Rules`.
- Multiple values in a table row can be changed with **one** command, for example in the rules table of the IPv4 firewall:
  - `set WINS UDP` sets the protocol of the WINS rule to UDP
  - `set WINS UDP ANYHOST` sets the protocol of the WINS rule to UDP and the destination to ANY-HOST
  - `set WINS * ANYHOST` also sets the destination of the WINS rule to ANYHOST; the asterisk means that the protocol remains unchanged
- 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. For example, in the rules table of the firewall, the destination has the number 4:
  - `set WINS {4} ANYHOST` sets the destination of the WINS rule to ANYHOST
  - `set WINS {destination} ANYHOST` also sets the destination of the WINS rule to ANYHOST
  - `set WINS {dest} ANYHOST` sets the destination of the WINS rule to ANYHOST, because specifying `dest` here is sufficient to uniquely identify the column name.
- 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, `ping ?` shows the options of the integrated ping command.
- Enter `help` or `?` on the command line for a complete listing of the available shell commands.

Parameter overview for the ping command

The ping command entered at the command prompt of a Telnet or terminal connection sends an "ICMP echo-request" packet to the destination address of the host to be checked. If the receiver supports the protocol and it is not filtered out in the firewall, the destination host will respond with an "ICMP echo reply". If the target computer is not reachable, the last device before the host responds with a "network unreachable" or "host unreachable" message.

The syntax of the ping command is as follows:

```
ping [-46dfnoqrmb] [-s n] [-i n] [-c n] [-x x][-p <dscp>][-a ...] destination [%scope] [%scope@rtg-tag]
[%%interface] [@rtg-tag]
```

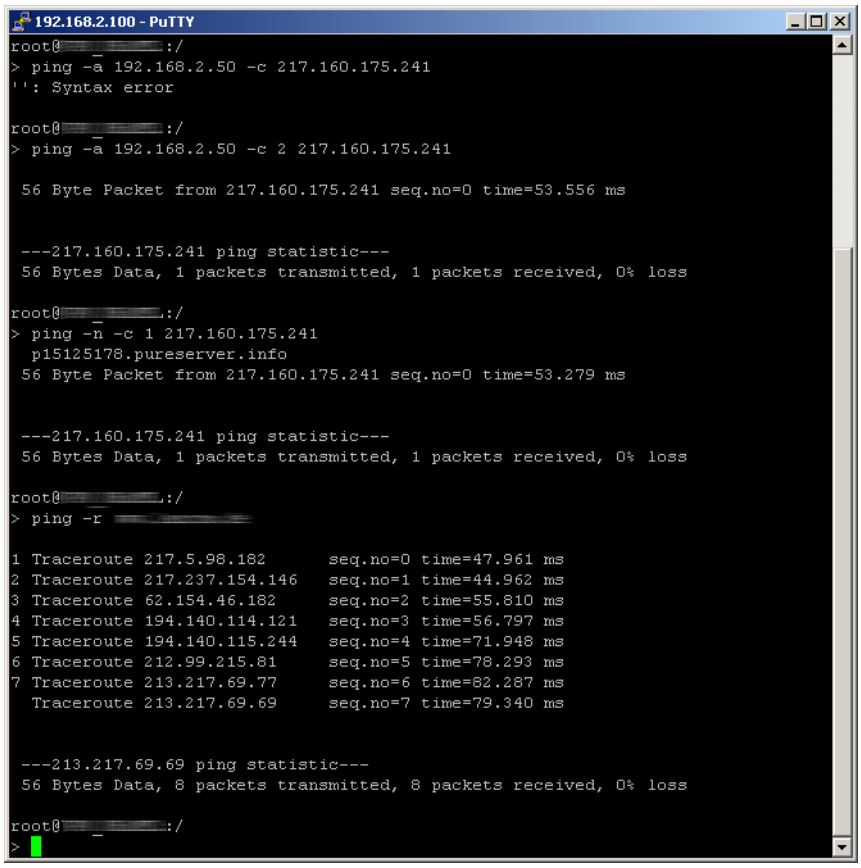
The meaning of the optional parameters is explained in the following table:

Table 2: Overview of optional parameters for the ping command

Parameter	Meaning
`-4`	Force IPv4
`-6`	Force IPv6

Parameter	Meaning
`-d`	Forbid fragmentation
`-f`	flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example. It is easy for flood ping to be misinterpreted as a denial-of-service (DoS) attack.
`-n`	Returns the computer name of a specified IP address.
`-o`	Immediately sends another request after a response.
`-q`	Ping command returns no output to the CLI (quiet).
`-r`	Switches to the traceroute mode. The path taken by the data packets to the target computer is displayed with all intermediate stations.
`-m`	Switches to the tracepath mode to determine the path MTU to the specified IP address.
`-b`	Do not stop pinging after receiving a PacketTooBig (DF), in order to achieve “Path MTU Discovery”.
`-s n`	Sets the packet size to n bytes (max. 65500).
`-i n`	Time between packets in seconds.
`-c n`	Send n pings.
`[-x x]`	Atomic fragments: (n)ever, (f)orce, (a)utomatic
`[-p <dscp>]`	Use a specific DSCP value for this ping. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible DSCP values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF
`-a a.b.c.d`	Sets the ping's sender address (default: IP address of the device.
`-a <name>`	Uses a named network, interface, or loopback address as the sender address
`-l <Load-Balancer-Policy>`	If the ping target is reached via a load balancer, the policy makes a load-balancer decision when the pings are sent. Possible values are default, traffic, bandwidth, round-robin, mst-used and all defined Dynamic Path Selection policies. If an invalid policy is specified, no pings are sent It is not possible to use this CLI option in combination with the specification of a scope or an interface binding in the destination.
`-6 <IPv6-Address>%<Scope>`	Performs a ping command to the link-local address via the interface specified by <scope>. For IPv6, the scope of parameters is of central importance: IPv6 requires a link-local address (fe80::/10) to be assigned to every network interface (logical or physical) on which the IPv6 protocol is enabled, so you must specify the scope when pinging a link-local address. This is the only way that the ping command knows which interface it should send the packet to. A percent sign (%) separates the name of the interface from the IPv6 address. **Examples:** › `ping -6 fe80::1%INTRANET` Pings the link-local address “fe80::1”, which is accessible via the interface and/or the network “INTRANET”.

Parameter	Meaning
	`> ping -6 2001:db8::1` Pings the global IPv6 address “2001:db8::1”.
`destination`	Address or host name of the target computer
`%scope`	Name of the interface used to send the packet when link-local addresses are used as the destination.
`%scope@rtg-tag`	Name of the interface used to send the packet when link-local addresses are used as the destination, with additional specification of the routing tag.
`%%interface`	Name of the destination interface. The packet is sent directly to the interface without taking the routing table into account.
`@rtg-tag`	Routing tag used to send the packet.
`stop /<RETURN>`	Entering `stop` or pressing the RETURN button terminates the ping command.



Parameter overview for the trace command

The traces available for a particular model can be displayed by the CLI by entering `trace` without any arguments.

Table 3: Overview of some executable traces

This parameter ...	...causes the following message in the trace:
`Status`	Connection status messages

This parameter ...	...causes the following message in the trace:
`Error`	Connection error messages
`ACME`	Automatic Certificate Management Environment (ACME) client
`ADSL`	ADSL connection status
`ARP`	Address resolution protocol
`ATM-cell`	ATM packet layer
`ATM-error`	ATM error
`Bridge`	Information on the wireless LAN bridge
`Connact`	Messages from the activity protocol
`Cron`	Activities of the scheduler (cron table)
`D-channel-dump`	Traces the D channel of the ISDN bus connected
`DFS`	Trace on dynamic frequency selection, automatic channel selection in the 5 GHz wireless LAN band
`DHCP`	Dynamic host configuration protocol
`DNS`	Domain name service protocol
`EAP`	Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1X
`Ethernet`	Information on the Ethernet interfaces
`Firewall`	Displays firewall events
`FW-DNS`	Changes to the firewall database of DNS destinations: › If a DNS packet arrives, it outputs the packet along with the affected wildcard expressions and destinations. › If the TTL (time-to-live) of an entry expires, it outputs the associated record along with the relevant wildcard expressions and destinations. › If one of the two firewalls registers or de-registers a DNS destination because its configuration has changed. › If there is a change to the table **Set up** > **Firewall** > **DNS-Destinations** or **Set up** > **Firewall** > **DNS-Destination-List**.
`GRE`	Messages to GRE tunnels
`hnat`	Information on hardware NAT
`IAPP`	Trace on inter access point protocol giving information on wireless LAN roaming.
`ICMP`	Internet control message protocol
`IGMP`	Information on the Internet group management protocol
`IP-masquerading`	Events in the masquerading module
`IPv6-config`	Information about the IPv6 configuration
`IPv6-firewall`	IPv6 firewall events
`IPv6-Interfaces`	Information about the IPv6 interfaces
`IPv6-LAN-Packet`	Data packets over the IPv6 LAN connection

This parameter ...	...causes the following message in the trace:
IPv6-router	Information about the IPv6 routing
IPv6-WAN-Packet	Data packets over the IPv6 WAN connection
L2TP	L2TPv2 / v3 protocol
LANAUTH	LAN authentication (e.g. Public Spot)
Load-balancer	Information on load balancing
Mail-client	E-mail processing by the internal mail client
VPN-Mesh	Trace for LANCOM Advanced Mesh VPN (AMVPN).
NETFLOW-Common	For more information about NetFlow/IPFIX, please see Reference manual.
NETFLOW-Error	
NETFLOW-Export	
NETFLOW-Metering	
NTP	Timeserver trace
Packet-dump	Displays the first 64 bytes of a packet in hexadecimal
PPP	PPP protocol negotiation
RADIUS	RADIUS trace
RIP	IP routing information protocol
Script	Script negotiation
Serial	Information on the state of the serial interface
SIP-packet	SIP information that is exchanged between a VoIP router and a SIP provider or an upstream SIP telephone system
SMTP-client	E-mail processing by the internal mail client
SNTP	Simple network time protocol
Spgtree	Information on spanning tree protocol
USB	Information on the state of the USB interface
VLAN	Information on virtual networks
VPN-packet	IPSec and IKE packets
VPN-status	IPSec and IKE negotiations
VRRP	Information on the virtual router redundancy protocol
Wireless-LAN	Information on activity in the wireless networks
WLAN-ACL	Status messages about MAC filtering rules. The display depends on how the WLAN data trace is configured. If a MAC address is specified there, the trace shows only the filter results relating to that specific MAC address.
XML-Interface-PbSpot	Messages from the Public Spot XML interface

Overview of CAPWAP parameters with the show command

The following information about the CAPWAP service can be viewed using the command line:

Table 4: Overview of all CAPWAP parameters with the show command

Parameters	Meaning
`-addresses [<IfcNum>]`	Shows the address tables of an individual or all WLC tunnels. In the case of an individual WLC tunnel, enter for the `<IfcNum>` the number of logical WLC tunnel interface, for example `10`.
`-groups`	Shows the information for an individual or all available assignment/tag groups.

You can supplement the command `show capwap groups` with the parameters listed below, which control the scope of the displayed information:

Table 5: Overview of all CAPWAP group parameters with the show command

Parameters	Meaning
`all`	Shows the names configured in the setup menu and the device's internal names for all assignment/tag groups as well as the default groups that were set up. The default group represents an internal group which contains all APs.
`<group1> <group2> <...>`	Shows all APs of the respective assignment/tag groups.
`-l <location>`	Shows all APs of the respective location.
`-c <country>`	Shows all APs of the respective country.
`-i <city>`	Shows all APs of the respective city.
`-s <street>`	Shows all APs of the respective street.
`-b <building>`	Shows all APs of the respective building.
`-f <floor>`	Shows all APs of the respective floor.
`-r <room>`	Shows all APs of the respective room description.
`-d <device>`	Shows all APs that have the specified device name.
`-v <firmware>`	Shows all APs which have the specified firmware. To do this, enter the version number for `<firmware>` followed by the build number, e.g., `9.00.0001`.
`-x <firmware>`	Shows all APs with a firmware version lower than the one installed on the current device.
`-y <firmware>`	Shows all APs with a firmware version the same or lower than the one installed on the current device.
`-z <firmware>`	Shows all APs with a firmware version higher than the one installed on the current device.
`-t <firmware>`	Shows all APs with a firmware version the same or higher than the one installed on the current device.
`-n <intranet>`	Shows all APs with an IP belonging to the specified Intranet address.
`-p <profile>`	Shows all APs that have been assigned with the specified WLAN profile.

Parameters	Meaning
`rmgrp <group1 intern_name> <group2 intern_name> …`	Deletes the group(s) with the specified internal names from the memory of the device. Use this command to free up the main memory if too large a number of groups is degrading the performance of the device. The entry in the setup menu is unaffected by this action.
`resetgrps`	Deletes all groups except the default group.

For location information the device evaluates the information entered under **Location** in the access point table. The following field names are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

For instance, the location entry `co=Germany, ci=Aachen` allows you to list all of the managed APs in Aachen from the console of the WLC with the command `+show capwap group -i Aachen`.

Example commands

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```

Overview of IPv6-specific show commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- *IPv6 addresses*: `show ipv6-addresses`
- *IPv6 prefixes*: `show ipv6-prefixes`
- *IPv6 interfaces*: `show ipv6-interfaces`
- *IPv6 neighbor cache*: `show ipv6-neighbour-cache`
- *IPv6 DHCP server* `show dhcp6-server`
- *IPv6 DHCP client* `show dhcpv6-client`
- *IPv6 route*: `show ipv6-route`

Additionally, IPv6 communications can be followed with the `trace` command.

IPv6 addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80:`.

The output is formatted as follows:

```
<Interface> :
<IPv6 address>, <status>, <attribute>, (<type>)
```

Table 6: Components of the command-line output `show ipv6-addresses`

Output	Comment
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	The status field can contain the following values: › TENTATIVE Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. › PREFERRED The address is valid › DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. › INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	Shows an attribute of the IPv6 address. Possible attributes are: › None No special attributes › (ANYCAST) This is an anycast address › (AUTO CONFIG) The address was retrieved by auto-configuration › (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

IPv6 prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

Delegated prefixes

All prefixes that the router has obtained by delegation.

Advertised prefixes

All prefixes that the router announces in its router advertisements.

Deprecated prefixes

All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

IPv6-Interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

<Interface> : <Status>, <Forwarding>, <Firewall>

Table 7: Components of the command-line output `show ipv6-interfaces`

Output	Comment
Interface	The name of the interface
Status	The status of the interface Possible entries are: › oper status is up › oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: › forwarding is enabled › forwarding is disabled
Firewall	The status of the firewall. Possible entries are: › forwarding is enabled › firewall is disabled

IPv6 neighbor cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

```
<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>
```

Table 8: Components of the command-line output `show ipv6-neighbor-cache`

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)
Status	The status of the connection to neighboring devices. Possible entries are: › INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. › REACHABLE The neighbor was reached in the last ten seconds. › STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. › DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols. › PROBE

Output	Comment
	The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.
Source	The IPv6 address at which the neighbor was detected.

IPv6 DHCP server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

IPv6 DHCP client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and which prefixes and DNS server it is using.

IPv6 route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

Environment variables

Environment variables are device-specific global variables with predefined values that you can insert anywhere on the command line as dynamic placeholders. An overview of the environment variables and their values can be output using the appropriate CLI commands (see below).

All predefined environment variables begin with two underscores: When entering commands on the command line, the variables are preceded by a dollar sign.

Table 9: Overview of all environment variables

Variable name	Contents
`__BLDDEVICE`	The sub-project of the device. The sub-project generally consists of a string without spaces and it stands for the hardware model of the current device.
`__DEVICE`	The type of the device, for example as displayed in LANconfig or on the device type label.
`__FWBUILD`	The build number of the firmware currently used in the device. The build number is a four-digit number
`__FWVERSION`	The version number of the firmware currently used in the device, in the form 'x.yy'. The firmware version consists of the major release before the dot and the minor release after it.
`__LDRBUILD`	The build number of the firmware currently operating in the device. The build number is a four-digit number
`__LDRVERSION`	The version number of the loader currently installed in the device, in the form 'x.yy'. The loader version consists of the major release before the dot and the minor release after it.
`__MACADDRESS`	The type of the device, given as a 12-digit string of hexadecimal values with lowercase letters and no separators.
`__SERIALNO`	The device serial number.
`__SYSNAME`	The system name of the device.

Use the following commands in the CLI to display or modify environment variables:

- `printenv`: Displays all environment variables and their current values. If you have set one or more environment variables with the command `setenv`, the output of the command `printenv` shows the user-defined value at the top and the default value below it.
- `echo $__device`: Displays the current values of a single environment variable, in this example the value for the variable '__DEVICE'.
- `setenv __device MeinWert`: Sets the value of an environment variable to the desired value.
- `unsetenv __device`: Sets the value of an environment variable to the default value.

Keyboard shortcuts for the command line

The following shortcuts can be used to edit the commands on the command line. The "ESC key sequences" show (for comparison) the shortcuts used on typical VT100/ANSI terminals:

Table 10: Overview of CLI keyboard shortcuts

Shortcut	Esc key sequences	Description
Up arrow	ESC [A	In the list of commands last run, jumps one position up (in the direction of older commands).
Down arrow	ESC [B	In the list of commands last run, jumps one position down (in the direction of newer commands).
Right arrow	Ctrl-F ESC [C	Moves the insert cursor one position to the right.
Left arrow	Ctrl-B ESC [D	Moves the insert cursor one position to the left.
Home or Pos1	Ctrl-A ESC [A ESC [1~ (	Moves the insert cursor to the first character in the line.
Close	Ctrl-E ESC [F ESC OF ESC [4~	Moves the insert cursor to the last character in the line.
Ins	ESC [ESC [2~	Switches between input and overwrite modes.
Del	Ctrl-D ESC <BS> ESC [3~	Deletes the character at the current position of the insert cursor or ends the Telnet session if the line is blank.
erase	<BS><DEL>	Deletes the next character to the left of the insert cursor.
erase-bol	Ctrl-U	Deletes all characters to the left of the insert cursor.
erase-eol	Ctrl-K	Deletes all characters to the right of the insert cursor.
Tabulator		Completes the input from the current position of the insert cursor for a command or path of the LCOS menu structure: **1.** If there is only one possibility of completing the command/path, this is accepted by the line. **2.** If there is more than one possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. Pressing the Tab key again displays a list of all possibilities to complete the entry. Then enter e.g. another letter, to allow unambiguous completion of the input. **3.** If there is no possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. No further actions are run. Further information on the special features of the Tab key for scripts can be found separately in the section *Tab command when scripting* on page 49,

Tab command when scripting

When working with scripts, the `tab` command enables the desired columns for the subsequent `set` command.

When you perform the configuration with a command line tool, you generally supplement the set command with the values for the columns of the table.

For example, you set the values for the performance settings of a WLAN interface as follows:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?

Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 Chars from: 1234567890

> set WLAN-1 Yes *
```

In this example the Performance table has three columns:

- Ifc, the desired interface
- Enable or disable QoS
- The desired value for TX bursting

With the command `set WLAN-1 Yes *` you enable the QoS function for WLAN-1, and you leave the value for TX bursting unchanged with the asterisk (*).

Working with the `set` command in this way is adequate for tables with only a few columns. However, tables with many columns can pose a major challenge. For example, the table under **Setup** > **Interfaces** > **WLAN** > **Transmission** contains 22 entries:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?

Possible Entries for columns in Transmission:
[1][Ifc]                 : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17), WLAN-1-4 (18), WLAN-1-5 (19), WLAN-1-6
(20), WLAN-1-7 (21), WLAN-1-8 (22)
[2][Packet-Size]         : 5 Chars from: 1234567890
[3][Min-Tx-Rate]        : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[9][Max-Tx-Rate]        : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[4][Basic-Rate]         : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M
 (13), 48M (14), 54M (15)
[19][EAPOL-Rate]        : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11),
 24M (12), 36M (13), 48M (14), 54M (15), HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35), HT-2-13M (36), HT-2-26M (37),
HT-2-39M (38), HT-2-52M (39), HT-2-78M (40), HT-2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]       : 3 Chars from: 1234567890
[11][Soft-Retries]       : 3 Chars from: 1234567890
[7][11b-Preamble]        : Auto (0), Long (1)
[16][Min-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[17][Max-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[23][Use-STBC]           : No (0), Yes (1)
[24][Use-LDPC]           : No (0), Yes (1)
[13][Short-Guard-Interval]  : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]    : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
[20][Max-Aggr.-Packet-Count]    : 2 Chars from: 1234567890
[6][RTS-Threshold]       : 5 Chars from: 1234567890
[10][Min-Frag-Len]       : 5 Chars from: 1234567890
[21][ProbeRsp-Retries]  : 3 Chars from: 1234567890
```

Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
> set WLAN-1-3 * * * * * * * * * * * * No
```

The asterisks for the values after the column for the short guard interval are unnecessary in this example, as the columns will be ignored when setting the new values.

As an alternative to this rather confusing and error-prone notation, you can use the `tab` command as the first step to determine which columns are changed with the subsequent `set` command:

```
> tab Ifc short guard-Interval
> set WLAN-1-3 No
```

The `tab` command also makes it possible to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
> tab Ifc short guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```

The tables may only contain only a selection of the columns, depending on the hardware model. The `tab` command ignores columns which do not exist for that device. This gives you the option to develop unified scripts for different hardware models. The `tab` instructions in the scripts reference the maximum number of required columns. Depending on the model, the script only performs the `set` instructions for the existing columns.

You can also abbreviate the `tab`command with curly brackets. Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
> set WLAN-1-3 {short-guard} No
```

The curly brackets also enable you to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
> set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

Function keys for the command line

The function keys (the F keys on the keyboard) allow users to save frequently used command sequences and to call them easily from the command line.

This function is configured in the Setup menu under **Config** > **Function-Keys**. Use thedrop-down menu under **Key** to select one of the function keys F1 to F12 and, under **Mapping**, enter the command sequence just as you would on the command line. You can enter any of the commands/shortcuts possible on the LCOS command line.

Special features of the caret character

When using the caret character (^) in your commands, be aware that this is also used to map special control commands with ASCII values below 32:

- ^A stands for Ctrl-A (ASCII 1)
- ^Z stands for Ctrl-Z (ASCII 26)
- ^[stands for Escape (ASCII 27)
- ^^ A double caret symbol stands for the caret symbol itself.

If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. By entering `caret + A`, the Windows operating system outputs an Â. To enter the caret character itself, enter a space in front of the subsequent characters. The sequence ^A is thus formed from `caret character + space + A`.

Character set for sending SMS

An SMS can contain a maximum of 160 characters (each of 7 bits = 1,120 bits). These are made up of the GSM basic character set (total of 128 characters) as well as selected characters from the extended GSM character set. Although the extended character set allows the use of some additional characters, these take up twice the space and correspondingly

reduce the maximum number of characters that the SMS can contain. Characters not implemented in the SMS module are ignored by the device.

The following characters are defined in the **GSM basic character set**:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" in the overview refers to the space character. "LF", "CR" and "ESC" refer to the control characters for the line feed, the carriage return and the escape in the extended GSM character set.

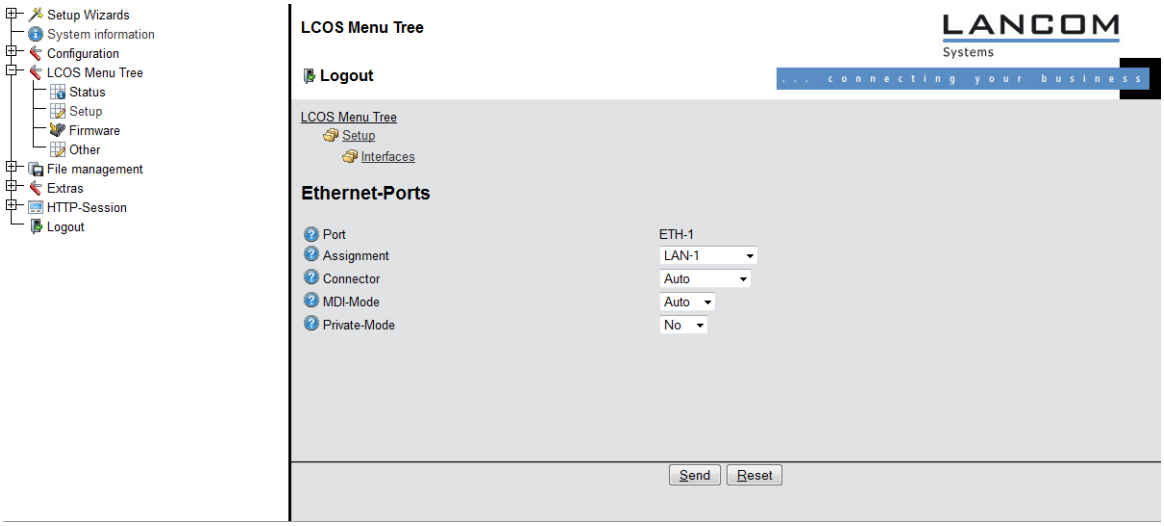
The following characters are implemented from the **extended GSM character set**:

{ | } [ ] ~ ^ \ €

1.4 Configuration with WEBconfig

Device settings can be configured from any Web browser. The device contains an integrated configuration software called WEBconfig. All you need to work with WEBconfig is a web browser. In a network with a DHCP server, you can access the device simply by entering its IP address into your web browser.

Menu area “LCOS Menu Tree” provides the configuration parameters in the same structure as they are used under Telnet. Clicking the question mark calls up help for each configuration parameter.



2 Setup

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

2.1 Name

This field can be used to enter a name of your choice for this device.

Console path:

Setup

Possible values:

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

Default:

empty

2.2 WAN

This menu contains the configuration of the Wide Area Network (WAN).

Console path:

Setup

2.2.2 Dialup-Peers

Here you configure the ISDN remote sites that your device is to connect to and exchange data with.

If two remote-site lists contain identical names for remote sites (e.g. DSL broadband remote sites and Dialup peers), the device automatically takes the "fastest" interface when establishing the connection. The other interface is available for backup purposes. If the list does not specify DSL broadband remote sites, access concentrators or services, then the device connects to the first AC that responds to the request over the exchange. For an existing DSLoL interface, the same entries apply as for a DSL interface. This information is entered into the list of DSL broadband remote sites.

Console path:

Setup > **WAN**

2.2.2.1 Remote site

Enter the name of the remote site here.

Console path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

Select from the list of defined peers.

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

Default:

empty

2.2.2.2 Dialup remote

A telephone number is only required if the remote is to be called. The field can be left empty if calls are to be received only. Several numbers for the same remote can be entered in the round-robin list.

Console path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

Max. 31 characters from `0123456789S*#-EF:`

Default:

empty

2.2.2.3 B1-DT

The connection is terminated if it remains unused for the time set here.

Console path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

0 … 9999

Default:

0

2.2.2.5 Layer name

From the layer list, select an entry that is to be used for this remote site.

The layer list already contains a number of entries with popular standard settings.

Console path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

Select from the list of defined layers

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

Default:

empty

2.2.2.8 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

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

Default:

DEFAULT

2.2.4 Layer

Here you collect individual protocols into 'layers' that are to be used to transfer data to other routers.

Console path:

Setup > **WAN**

2.2.4.1 Layer name

This name is used for selecting the layer in the list of remote stations.

Console path:

Setup > **WAN** > **Layer**

Possible values:

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

Default:

empty

2.2.4.2 Encaps.

Additional encapsulations can be set for data packets.

Console path:

Setup > **WAN** > **Layer**

Possible values:

TRANS

Transparent: No additional encapsulation

ETHER

Ethernet: Encapsulation as Ethernet frames.

LLC-MUX

Multiplexing via ATM with LLC/SNAP encapsulation as per RFC 2684. Several protocols can be transmitted over the same VC (virtual channel).

VC-MUX

Multiplexing via ATM by establishing additional VCs as per RFC 2684.

Default:

ETHER

2.2.4.3 Lay-3

The following options are available for the network layer:

Console path:

Setup > **WAN** > **Layer**

Possible values:

PPP

The connection is established according to the PPP protocol (in synchronous mode, i.e. bit oriented). The configuration data are taken from the PPP table.

DHCP

Assignment of network parameters by DHCP.

B-DHCP

The connection is established with DHCP client and broadcast flag set in DHCP.

TRANS

Transparent: No additional header is inserted.

Default:

PPP

2.2.4.4 Lay-2

This field configures the upper sublayer of the data link layer.

Console path:

Setup > **WAN** > **Layer**

Possible values:

PPPoE

PPP over Ethernet: PPP information is encapsulated in Ethernet frames

TRANS

Transparent: No additional header is inserted.

Default:

TRANS

2.2.4.6 Lay-1

This field is used to configure the lower section of the security layer (the data link layer) for the WAN layer.

The range of available values depends on the hardware model at hand.

Console path:

Setup > **WAN** > **Layer**

Possible values:

ETH

Transparent Ethernet as per IEEE 802.3.

VDSL

VDSL2 data transmission as per ITU G.993.2.

WWAN

For connections via the internal WWAN modem.

XDSL

For connections via the internal XDSL modem.

Default:

ETH

2.2.5 PPP

In order for the device to be able to establish PPP or PPTP connections, you must enter the corresponding parameters (such as name and password) for each remote site into this list.

Console path:

Setup > **WAN**

2.2.5.1 Remote-Site

Enter the name of the remote site here. This name has to agree with the entry in the list of peers/remote sites. You can also select a name directly from the list of peers / remote sites.

Console path:

Setup > **WAN** > **PPP**

Possible values:

Select from the list of defined peers.

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

Default:

empty

Possible values:

Special values:

DEFAULT

During PPP negotiations, a remote site dialing-in to the device logs on with its name. The device can use the name to retrieve the permitted values for authentication from the PPP table. At the start of the negotiation, the remote site occasionally cannot be identified by IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

2.2.5.2 Authent.request

Method for securing the PPP connection that the device expects from the remote site.

Console path:

Setup > **WAN** > **PPP**

Possible values:

MS-CHAPv2
MS-CHAP
CHAP
PAP

2.2.5.3 Password

Password transferred from your device to the remote site (if required). A '*' in the list indicates that an entry exists.

Console path:

Setup > **WAN** > **PPP**

Possible values:

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

Default:

empty

2.2.5.4 Time

Time between two tests of the connection with LCP (see also LCP). This time is entered in multiples of 10 seconds (e.g. 2 for 20 seconds). The value is also the time between two tests of the connection as per CHAP. This time is entered in minutes. For remote sites running the Windows operating system the time must be set to 0.

Console path:

Setup > **WAN** > **PPP**

Possible values:

0 … 99

Default:

0

2.2.5.5 Try

Number of retries for the test attempt. Multiple retries reduces the impact from temporary line faults. The connection is only terminated if all tries prove unsuccessful. The time between two retries is one tenth (1/10) of the time between two tests. This value is also the maximum number of "Configure Requests" that the device sends before assuming a line fault and tearing down the connection itself.

Console path:

Setup > **WAN** > **PPP**

Possible values:

0 … 99

Default:

5

2.2.5.6 User name

Name with which your device logs in to the remote site. If there is no entry here, your device's device name is used.

Console path:

Setup > **WAN** > **PPP**

Possible values:

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

Default:

empty

2.2.5.7 Conf

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information on fault rectification. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Console path:

Setup > **WAN** > **PPP**

Possible values:

0 … 255

Default:

10

2.2.5.8 Fail

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information on fault rectification. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Console path:

Setup > **WAN** > **PPP**

Possible values:

0 … 255

Default:

5

2.2.5.9 Term

This parameter affects the mode of operation of the PPP. The parameter is defined in RFC 1661 and is not described in further detail here. If you are unable to establish PPP connections, this RFC in conjunction with the PPP statistics of the router provides information. The default settings are generally sufficient. This parameter can only be changed with LANconfig, SNMP or TFTP.

Console path:

Setup > **WAN** > **PPP**

Possible values:

0 … 255

Default:

2

2.2.5.10 Rights

Specifies the protocols that can be routed to this remote site.

Console path:

Setup > **WAN** > **PPP**

Possible values:

IP
IPX
IP+IPX

Default:

IP

2.2.5.11 Authent-response

Method for securing the PPP connection that the device offers when dialing into a remote site.

The device only uses the protocols enabled here—other negotiations with the remote site are not possible.

Console path:

Setup > **WAN** > **PPP**

Possible values:

MS-CHAPv2
MS-CHAP
CHAP
PAP

Default:

MS-CHAPv2

MS-CHAP

CHAP

PAP

2.2.13 Manual dialing

This menu contains the settings for manual dialing.

Console path:

Setup > **WAN**

2.2.13.1 Establish

Establishes a connection to the remote site which is entered as a parameter.

Console path:

Setup > **WAN** > **Manual dialing**

Possible arguments:

<Remote>

Name of a remote site defined in the device.

2.2.13.2 Disconnect

Terminates a connection to the remote site which is entered as a parameter.

Console path:

Setup > **WAN** > **Manual dialing**

Possible arguments:

<Remote>

Name of a remote site defined in the device.

2.2.15 Keepalive-without-Route

Specifies whether a connection to a remote site, e.g. a VPN tunnel or an Internet connection, should be established even without a route. Connecting to the remote site without an explicit route in the routing table is necessary if the remote site transmits the routes, e.g. by DHCP (Classless Static Route Option) or a dynamic routing protocol.

Console path:

Setup > **WAN**

Possible values:

No

Connects to remote sites only when a route exists. This corresponds to the default behavior up until LCOS 10.40.

Yes

As of LCOS 10.40 this option allows connections to remote sites even without an existing route.

Default:

No

2.2.18 Backup-Delay-Seconds

Wait time before establishing a backup connection in case a remote site should fail.

The backup timer also controls the VRRP switchover time.

Console path:

Setup > **WAN**

Possible values:

0 … 9999 Seconds

Default:

30

2.2.19 DSL-Broadband-Peers

Here you configure the DSL broadband remote sites that your device is to connect to and exchange data with.

Console path:

Setup > **WAN**

2.2.19.1 Remote site

Enter the name of the remote site here.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Select from the list of defined peers.

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

Default:

empty

2.2.19.3 SH-Time

This is where you define the number of seconds of inactivity after which the connection to this remote site is to be closed.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

0 … 9999

Special values:

9999

Ensures an immediate connection without time limits.

2.2.19.5 Layer name

Select the communication layer to be used for this connection. How to configure this layer is described in the following section.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

empty

2.2.19.9 AC-Name

The parameters for 'Access Concentrator' and 'Service' are used to explicitly identify the Internet provider. These parameters are communicated to you by your Internet provider.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

empty

2.2.19.10 Service name

The parameters for 'Access Concentrator' and 'Service' are used to explicitly identify the Internet provider. These parameters are communicated to you by your Internet provider.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

empty

2.2.19.11 ATM-VPI

Enter the VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) for your ADSL connection here. These values are communicated to you by your ADSL network operator. Typical values for VPI/VCI are, for example: 0/35, 0/38, 1/32, 8/35, 8/48.

Console path:

Setup > **WAN** > **DSL-Broadband-Peer**

Possible values:

0 … 999

Default:

0

2.2.19.12 ATM-VCI

Enter the VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) for your ADSL connection here. These values are communicated to you by your ADSL network operator. Typical values for VPI/VCI are, for example: 0/35, 0/38, 1/32, 8/35, 8/48.

Console path:

Setup > **WAN** > **DSL-Broadband-Peer**

Possible values:

0 … 99999

Default:

0

2.2.19.13 user-def.-MAC

Enter the MAC address of your choice is a user-defined address is required.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

000000000000

2.2.19.14 DSL-Ifc(s)

Enter the port number of the DSL port here. It is possible to make multiple entries. Separate the list entries either with commas (1,2,3,4) or divide it into ranges (1-4). Activate channel bundling in the relevant layer to bundle the DSL lines.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Max. 8 characters from `-,01234`

Default:

0

2.2.19.15 MAC-Type

Here you select the MAC addresses which are to be used.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Global

If 'Global' is selected, the device MAC address is used for all connections.

Local

If 'Local' is selected, the device MAC addresses are used to form further virtual addresses for each WAN connection.

user-def.

If a certain MAC address (user defined) is to be defined for the remote site, this can be entered into this field.

Default:

Local

2.2.19.16 VLAN-ID

Here you enter the specific ID of the VLAN to identify it explicitly on the DSL connection.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

0 … 4096

Default:

0

2.2.19.17 Prio-Mapping

This entry controls how the priority mapping functions.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Off

Prio-mapping is disabled.

1TR-112

The value "1TR112" maps the precedence (i.e., the top 3 bits) of the DSCP into the VLAN priority field. Additionally, PPP-LCP echo packets are marked with VLAN priority 6, and IGMP packets are marked with 4.

DSCP

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

Value

All packets sent to the WAN are marked with the priority tag configured under *2.2.19.20 Prio-Value* on page 68. However, this only happens if a VLAN other than 0 is also configured. Otherwise it would be equivalent to being set to "Off".

Default:

Off

2.2.19.19 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

DEFAULT

2.2.19.20 Prio-Value

This value is set as the VLAN priority value when *2.2.19.17 Prio-Mapping* on page 68 is set to "Value".

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

0 … 7

2.2.19.21 S-VLAN-ID

Here you configure the S-VLAN for VLAN double tagging (Q-in-Q VLAN connections according to IEEE 802.1ad). The VLAN is also referred to as the outer VLAN. The S-VLAN protocol ID that is used can be configured under *2.32.6 S-Tag-Value* on page 1057.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

0 … 4096

Default:

0

2.2.19.22 PPPoE-MTU-1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

Console path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Yes
No

Default:

No

2.2.20 IP-List

If certain remote sites do not automatically transmit the IP parameters needed for a connection, then enter these values here.

Use this table to configure the extranet address of a VPN tunnel, for example.

Console path:

Setup > **WAN**

2.2.20.1 Remote site

Enter the name for the remote station here.

When configuring a VPN tunnel, this entry corresponds to the appropriate service under **Setup** > **VPN** > **VPN-Peers** or **Setup** > **VPN** > **IKEv2** > **Connections**.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

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

Default:

empty

2.2.20.2 IP address

If your Internet provider has supplied you with a fixed, publicly accessible IP address, you can enter this here. Otherwise leave this field empty. If you use a private address range in your local network and the device is to be assigned with one of these addresses, do not enter the address here but under intranet IP address instead.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.20.3 IP-Netmask

Specify here the netmask associated with the address above.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.20.4 Gateway

Enter the address of the standard gateway here.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.20.5 DNS-Default

Specify here the address of a name server to which DNS requests are to be forwarded. This field can be left empty if you have an Internet provider or other remote site that automatically assigns a name server to the device when it logs in.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.20.6 DNS-Backup

Specify here a name server to be used in case the first DNS server fails.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.20.9 Masq.-IP-Addr.

Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned you static IP addresses, or if you wish to operate masquerading for your VPN network, you assign it to the respective connection here. If the masquerading IP address is not set, then the address assigned when the connection was established is used for masquerading.

You need to set a masquerading address for a VPN connection if you wish to mask a private network behind this address in the VPN network.

This setting is also necessary if a private address (172.16.x.x) is assigned during PPP negotiation. Normal masquerading is thus impossible as this type of address is filtered in the Internet.

Console path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.2.21 PPTP peers

This table displays and adds the PPTP remote sites.

Console path:

Setup > **WAN**

2.2.21.1 Remote site

This name from the list of DSL broadband peers.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

Select from the list of defined peers.

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

Default:

empty

2.2.21.3 Port

IP port used for running the PPTP protocol. According to the protocol standard, port '1,723' should always be specified.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

0 … 99999

Default:

0

2.2.21.4 SH time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

0 … 3600 Seconds

Default:

0

Special values:

9999

Connections are established immediately and without a time limit.

2.2.21.5 Rtg-Tag

Routing tag for this entry.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

0 … 65535

Default:

0

2.2.21.6 IP address

Specify the IP address of the PPTP remote station here.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

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

Default:

empty

2.2.21.7 Encryption

Here you enter the key length.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

Off
40-Bits
56-Bits
128-Bits

Default:

Off

2.2.21.9 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **WAN** > **PPTP-peers**

Possible values:

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

Default:

DEFAULT

2.2.22 RADIUS

This menu contains the settings for the RADIUS server.

Console path:

Setup > **WAN**

2.2.22.1 Operating

Switches RADIUS authentication on/off.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No
Yes
Exclusive

Default:

No

2.2.22.3 Auth.-Port

The TCP/UDP port over which the external RADIUS server can be reached.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

0 … 4294967295

Default:

1812

2.2.22.4 Key

Specify here the key (shared secret) of your RADIUS server from which users are managed centrally.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

Default:

0

2.2.22.5 PPP-Operation

When PPP remote sites dial in, the internal user authentication data from the PPP list, or alternatively an external RADIUS server, can be used for authentication.

If you switch the PPP mode to 'Exclusive', the internal user authentication data is ignored, otherwise these have priority.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

Yes

Enables the use of an external RADIUS server for authentication of PPP remote sites. A matching entry in the PPP list takes priority however.

No

No external RADIUS server is used for authentication of PPP remote sites.

Exclusive

Enables the use of an external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Default:

No

2.2.22.8 Loopback-Addr.

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address. If you have configured loopback addresses, you can specify them here as source address.

If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

Name of the IP network whose address should be used, or any valid IP address

Special values:

INT

for the address of the first intranet

DMZ

for the address of the first DMZ

LB0 to LBF

for the 16 loopback addresses

2.2.22.9 Protocol

RADIUS over UDP or RADSEC over TCP with TLS can be used as the transmission protocol for authentication on an external server.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.2.22.10 Auth.-Protocols

Method for securing the PPP connection permitted by the external RADIUS server. Do not set a method here if the remote site is an Internet provider that your device is to call.

If all methods are selected, the next available method of authentication is used if the previous one failed. If none of the methods are selected, authentication is not requested from the remote site.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

MS-CHAPv2
MS-CHAP
CHAP
PAP

Default:

MS-CHAPv2

MS-CHAP

CHAP

PAP

2.2.22.11 Server host name

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server to be used to centrally manage the users.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

Default:

empty

2.2.22.12 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

Default:

empty

2.2.22.20 L2TP-Operating

This item determines whether RADIUS should be used to authenticate the tunnel endpoint.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No

There is no RADIUS authentication.

Yes

RADIUS authentication occurs if, in the table 'L2TP Endpoints', the field 'Auth-Peer' is set to 'Yes', but no password was entered.

Exclusive

RADIUS authentication always occurs if, in the table 'L2TP Endpoints', the field 'Auth-Peer' is set to 'Yes', irrespective of whether a password was entered.

Default:

No

2.2.22.21 L2TP-Server-Hostname

IP address of the RADIUS server

The internal RADIUS server of the device does not support tunnel authentication. An external RADIUS server is required for this purpose.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

2.2.22.22 L2TP-Auth.-Port

The UDP port of the RADIUS server.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

0 … 65535

2.2.22.23 Loopback-Address

The sender address used for RADIUS requests.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

2.2.22.24 L2TP protocol

The protocol to be used.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.2.22.25 L2TP Secret

The shared secret between the device and the RADIUS server.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

2.2.22.26 L2TP password

The password stored together with the host in the RADIUS server. After authentication, the password for the tunnel is sent by the RADIUS server.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

2.2.22.27 L2TP attribute values

With this entry you configure the RADIUS attributes for the tunnel end point of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

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

Default:

empty

2.2.22.28 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.2.22.29 L2TP-Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.2.23 Polling table

In this table you can specify up to 4 IP addresses for non-PPP-based remote sites which are to be accessed for connection monitoring purposes.

Console path:

Setup > **WAN**

2.2.23.1 Remote site

Name of the remote site which is to be checked with this entry.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Select from the list of defined peers.

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

Default:

empty

2.2.23.2 IP-address-1

IP addresses for targeting with ICMP requests to check the remote site.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Valid IP address

Default:

0.0.0.0

2.2.23.3 Time

Enter the ping interval here.

If you enter 0 here and for the re-tries, the default values will be used.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

0 … 4294967295 Seconds

Default:

0

2.2.23.4 Try

If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

0 … 255

Default:

0

Special values:

0

Uses the default value of 5 retries.

2.2.23.5 IP-address-2

IP addresses for targeting with ICMP requests to check the remote site.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Valid IP address

Default:

0.0.0.0

2.2.23.6 IP-address-3

IP addresses for targeting with ICMP requests to check the remote site.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Valid IP address

Default:

0.0.0.0

2.2.23.7 IP-address-4

IP addresses for targeting with ICMP requests to check the remote site.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Valid IP address

Default:

0.0.0.0

2.2.23.8 Loopback-Addr.

Sender address sent with the ping; this is also the destination for the answering ping.

If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Name of the IP network whose address should be used, or any valid IP address

Special values:

INT

for the address of the first intranet

DMZ

for the address of the first DMZ

LB0 to LBF

for the 16 loopback addresses

2.2.23.9 Type

This setting influences the behavior of the polling.

Console path:

Setup > **WAN** > **Polling-Table**

Possible values:

Forced

The device polls in the given interval. This is the default behavior of LCOS versions <8.00, which did not yet have this parameter.

Auto

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

Default:

Forced

2.2.24 Backup peers

This table is used to specify a list of possible backup connections for each remote site.

Console path:

Setup > **WAN**

2.2.24.1 Remote site

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

Console path:

Setup > **WAN** > **Backup-Peers**

Possible values:

Select from the list of backup peers.

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

Default:

empty

2.2.24.2 Alternative peers

Specify here one or more remote sites for backup connections.

Console path:

Setup > **WAN** > **Backup-Peers**

Possible values:

Select from the list of backup peers.

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

Default:

empty

2.2.24.3 Head

Specify here whether the next connection is to be established to the number last reached successfully, or always to the first number.

Console path:

Setup > **WAN** > **Backup-Peers**

Possible values:

First
Last

Default:

Last

2.2.25 Action-Table

With the action table you can define actions that are executed when the status of a WAN connection changes.

Console path:

Setup > **WAN**

2.2.25.1 Index

The index gives the position of the entry in the table, and thus it must be unique. Entries in the action table are executed consecutively as soon as there is a corresponding change in status of the WAN connection. The entry in the field 'Check for' can be used to skip lines depending on the result of the action. The index sets the position of the entries in the table (in ascending order) and thus significantly influences the behavior of actions when the option 'Check for' is used. The index can also be used to actuate an entry in the action table via a cron job, for example to activate or deactivate an entry at certain times.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

1 … 4294967295

Default:

1

2.2.25.2 Host-Name

Action name. This name can be referenced in the fields *2.2.25.6 Action* on page 87 und *2.2.25.7 Check-For* on page 88 with the place holder `%h` (host name). Several entries with the same name are grouped together and the corresponding actions are executed one after the other.

The behavior for entries with an empty hostname is undefined!

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

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

2.2.25.3 Peer

A change in status of this remote site triggers the action defined in this entry.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Select from the list of defined peers.

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

Default:

empty

2.2.25.4 Lock-Time

Prevents this action from being repeated within the period defined here.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

0 … 4294967295 Seconds

Default:

0

2.2.25.5 Condition

The action is triggered when the change in WAN-connection status set here occurs.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Establish

The action is triggered when the connection has been established successfully.

Disconnect

The action is triggered when the device itself terminates the connection (e.g.by manual disconnection or when the hold time expires).

Close

The action is triggered on disconnection (whatever the reason for this).

Error

This action is triggered on disconnects that were not initiated or expected by the device.

Establish failure

This action is triggered when a connection establishment was started but not successfully concluded.

Default:

Establish

2.2.25.6 Action

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

Prefixes:

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

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

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

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

Optional variables for the actions:

- `%a` – WAN IPv4 address of the WAN connection relating to the action.

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

  The variable `%x` transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.
- `%y` – The current IPv6 LAN address of the device as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”.
- `%{yNetworkname}` – e.g. `%{yTESTNET}` for the current IPv6 LAN address of the device in the TESTNET network as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”.

  The variable `%y` transfers only the values of the network with the fixed name INTRANET. This can also be used to pass the LAN network name used for this variable.
- `%z` – WAN IPv6 address of the WAN connection relating to the action.
- `%H` – Host name of the WAN connection relating to the action.
- `%h` – Like `%H`, except the hostname is in small letters.
- `%c` – Connection name of the WAN connection relating to the action.
- `%n` – Device name
- `%s` – Device serial number
- `%m` – Device MAC address (as in Sysinfo)
- `%t` – Time and date in the format `YYYY-MM-DD hh:mm:ss`
- `%e` – Description of the error that was reported when connection establishment failed.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Max. 250 characters

Default:

empty

2.2.25.7 Check-For

The result of the action can be evaluated here to determine the number of lines to be skipped in the processing of the action table.

Prefixes/suffixes:

- contains= – This prefix checks if the result of the action contains the defined string.
- isequal= – This prefix checks if the result of the action is exactly equal to the defined string.
- ?skipiftrue= – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is TRUE.
- ?skipiffalse= – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is FALSE.

Optional variables for the actions:

- `%a` – WAN IPv4 address of the WAN connection relating to the action.

- `%x` – The current IPv6 LAN prefix as a string in the format “fd00:0:0:1::/64”
- `%y` – The current IPv6 LAN address of the device as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”
- `%z` – WAN IPv6 address of the WAN connection relating to the action.
- `%H` – Host name of the WAN connection relating to the action.
- `%h` – Like `%H`, except the hostname is in small letters.
- `%c` – Connection name of the WAN connection relating to the action.
- `%n` – Device name
- `%s` – Device serial number
- `%m` – Device MAC address (as in Sysinfo)
- `%t` – Time and date in the format `YYYY-MM-DD hh:mm:ss`
- `%e` – Description of the error that was reported when connection establishment failed.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Max. 50 characters

Default:

empty

2.2.25.8 Active

Activates or deactivates this entry.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Yes
No

Default:

Yes

2.2.25.9 Owner

Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the action will not be carried out.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

Select from the administrators defined in the device

Max. 16 characters

Default:

root

2.2.25.10 Routing-Tag

Routing tags are used to associate actions in the action table with a specific WAN connection. The device performs the action over the connection that is marked with this routing tag.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

0 … 65535

Default:

0

2.2.25.10 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

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

Default:

empty

2.2.26 MTU-List

This table allows you to set alternative MTU (Maximum Transfer Unit) values to those automatically negotiated by default.

Console path:

Setup > **WAN**

2.2.26.1 Peer

Enter the name of the peer here. This name must match an entry in the list of peers. You can also directly select a name from the list of peers.

You can use the wildcards "?" and "*" at any position in the peer name. "?" represents exactly one character. "*" represents any number of characters or none. The MTU list is sorted in descending order by the length of the peer name and, for names of the same length, in descending alphabetical order. This ensures that complete names always appear before names with wildcards.

Console path:

Setup > **WAN** > **MTU-List**

Possible values:

Selection from the list of defined peers

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

Default:

empty

2.2.26.2 MTU

Here you can manually define a maximum MTU per connection in addition to the automatic MTU settings. Enter the maximum IP packet length/size in bytes. Smaller values lead to greater fragmentation of the payload data.

Console path:

Setup > **WAN** > **MTU-List**

Possible values:

0 … 9999 Bytes

Default:

0

2.2.30 Additional PPTP gateways

Here you can define up to 32 additional gateways to ensure the availability of PPTP peers. Each of the PPTP peers has the possibility of using up to 33 gateways. The additional gateways can be defined in a supplementary list.

Console path:

Setup > **WAN**

2.2.30.1 Remote site

Here you select the PPTP remote site that this entry applies to.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Select from the list of defined PPTP remote stations.

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

Default:

empty

2.2.30.2 Begin with

Here you select the order in which the entries are to be tried.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Last used

Selects the entry for the connection which was successfully used most recently.

First

Selects the first of the configured remote sites.

Random

Selects one of the configured remote sites at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

Default:

Last used

2.2.30.3 Gateway -1

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.4 Rtg-Tag-1

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.5 Gateway -2

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.6 Rtg-Tag-2

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.7 Gateway -3

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.8 Rtg-Tag-3

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.9 Gateway -4

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.10 Rtg-Tag-4

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.11 Gateway -5

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.12 Rtg-Tag-5

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.13 Gateway -6

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.14 Rtg-Tag-6

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.15 Gateway -7

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.16 Rtg-Tag-7

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.17 Gateway -8

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.18 Rtg-Tag-8

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.19 Gateway -9

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.20 Rtg-Tag-9

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.21 Gateway -10

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.22 Rtg-Tag-10

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.23 Gateway -11

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.24 Rtg-Tag-11

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.25 Gateway -12

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.26 Rtg-Tag-12

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.27 Gateway -13

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.28 Rtg-Tag-13

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.29 Gateway -14

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.30 Rtg-Tag-14

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.31 Gateway -15

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.32 Rtg-Tag-15

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.33 Gateway -16

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.34 Rtg-Tag-16

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.35 Gateway -17

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.36 Rtg-Tag-17

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.37 Gateway -18

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.38 Rtg-Tag-18

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.39 Gateway -19

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.40 Rtg-Tag-19

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.41 Gateway -20

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.42 Rtg-Tag-20

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.43 Gateway -21

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.44 Rtg-Tag-21

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.45 Gateway -22

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.46 Rtg-Tag-22

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.47 Gateway -23

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.48 Rtg-Tag-23

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.49 Gateway -24

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.50 Rtg-Tag-24

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.51 Gateway -25

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.52 Rtg-Tag-25

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.53 Gateway -26

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.54 Rtg-Tag-26

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.55 Gateway -27

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.56 Rtg-Tag-27

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.57 Gateway -28

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.58 Rtg-Tag-28

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.59 Gateway -29

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.60 Rtg-Tag-29

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.61 Gateway -30

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.62 Rtg-Tag-30

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.63 Gateway -31

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.64 Rtg-Tag-31

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.30.65 Gateway -32

Enter the IP address of the additional gateway to be used for this PPTP remote station.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

Valid IP address, max. 63 characters

Default:

empty

2.2.30.66 Rtg-Tag-32

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **WAN** > **Additional-PPTP-Gateways**

Possible values:

0 … 65535

Default:

0

Special values:

0

The routing tag configured for this remote station in the PPTP connection list is taken for the associated gateway.

2.2.31 PPTP source check

With this entry you specify the basis used by the PPTP (point-to-point tunneling protocol) to check incoming connections.

Console path:

Setup > **WAN**

Possible values:

Address

The PPTP checks the address only. This is the standard behavior of older versions of LCOS without this parameter.

Tag+address

The PPTP checks the address and also the routing tag of interface to be used for the connection.

Default:

Address

2.2.35 L2TP 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:

Identifier: DEFAULT

Poll: 20

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 > **WAN**

2.2.35.1 Identifier

The name of the tunnel endpoint. If an authenticated L2TP tunnel is to be established between two devices, the entries 'Identifier' and 'Hostname' need to cross match.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

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

2.2.35.2 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 > **WAN** > **L2TP-Endpoints**

Possible values:

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

2.2.35.3 Rtg-Tag

The tag assigned to the route to the tunnel endpoint is specified here.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

0 … 65535

2.2.35.4 Port

UDP port to be used.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

0 … 65535

Default:

1701

2.2.35.5 Poll

The polling interval in seconds.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

0 … 65535

Default:

20

2.2.35.6 Host name

User name for the authentication If an authenticated L2TP tunnel is to be established between two devices, the entries 'Identifier' and 'Hostname' need to cross match.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

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

2.2.35.7 Password

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

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

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

2.2.35.8 Auth-Peer

Specifies whether the remote station should be authenticated.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

No
Yes

Default:

No

2.2.35.9 Hide

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

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

No
Yes

Default:

No

2.2.35.10 Source address

Here you can optionally specify a loopback address for the device to use as the target address instead of the one that would normally be selected automatically.

If the list of IP networks or source addresses contains an entry named 'DMZ', then the associated IP address will be used.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

Valid entry from the list of possible addresses.

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ

LB0 to LBF for the 16 loopback addresses

Any valid IP address

empty

Default:

2.2.35.11 Version

The L2TP protocol version used for this L2TP endpoint, either version 2 or 3.

Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

L2TPv2

Layer 2 Tunneling Protocol Version 2

L2TPv3

Layer 2 Tunneling Protocol Version 3

2.2.35.12 Operating

This L2TP endpoint is enabled or disabled.

Console path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

No

L2TP endpoint is disabled.

Yes

L2TP endpoint is enabled.

2.2.36 L2TP-Additional-Gateways

This table allows you to specify up to 32 redundant gateways for each L2TP tunnel.

Console path:

Setup > **WAN**

2.2.36.1 Identifier

The name of the tunnel endpoint as also used in the table of L2TP endpoints.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.2 Begin with

This setting specifies which redundant gateway is used first.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

Last used

This selects the last successfully used gateway.

First

This always selects the first gateway.

Random

A random gateway is selected at each attempt.

Default:

Last used

2.2.36.3 Gateway -1

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.4 Rtg-Tag-1

The routing tag of the route where Gateway-1 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.5 Gateway -2

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.6 Rtg-Tag-2

The routing tag of the route where Gateway-2 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.7 Gateway -3

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.8 Rtg-Tag-3

The routing tag of the route where Gateway-3 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.9 Gateway -4

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.10 Rtg-Tag-4

The routing tag of the route where Gateway-4 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.11 Gateway -5

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.12 Rtg-Tag-5

The routing tag of the route where Gateway-5 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.13 Gateway -6

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.14 Rtg-Tag-6

The routing tag of the route where Gateway-6 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.15 Gateway -7

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.16 Rtg-Tag-7

The routing tag of the route where Gateway-7 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.17 Gateway -8

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.18 Rtg-Tag-8

The routing tag of the route where Gateway-8 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.19 Gateway -9

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.20 Rtg-Tag-9

The routing tag of the route where Gateway-9 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.21 Gateway -10

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.22 Rtg-Tag-10

The routing tag of the route where Gateway-10 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.23 Gateway -11

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.24 Rtg-Tag-11

The routing tag of the route where Gateway-11 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.25 Gateway -12

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.26 Rtg-Tag-12

The routing tag of the route where Gateway-12 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.27 Gateway -13

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.28 Rtg-Tag-13

The routing tag of the route where Gateway-13 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.29 Gateway -14

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.30 Rtg-Tag-14

The routing tag of the route where Gateway-14 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.31 Gateway -15

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.32 Rtg-Tag-15

The routing tag of the route where Gateway-15 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.33 Gateway -16

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.34 Rtg-Tag-16

The routing tag of the route where Gateway-16 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.35 Gateway -17

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.36 Rtg-Tag-17

The routing tag of the route where Gateway-17 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.37 Gateway -18

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.38 Rtg-Tag-18

The routing tag of the route where Gateway-18 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.39 Gateway -19

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.40 Rtg-Tag-19

The routing tag of the route where Gateway-19 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.41 Gateway -20

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.42 Rtg-Tag-20

The routing tag of the route where Gateway-20 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.43 Gateway -21

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.44 Rtg-Tag-21

The routing tag of the route where Gateway-21 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.45 Gateway -22

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.46 Rtg-Tag-22

The routing tag of the route where Gateway-22 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.47 Gateway -23

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.48 Rtg-Tag-23

The routing tag of the route where Gateway-23 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.49 Gateway -24

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.50 Rtg-Tag-24

The routing tag of the route where Gateway-24 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.51 Gateway -25

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.52 Rtg-Tag-25

The routing tag of the route where Gateway-25 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.53 Gateway -26

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.54 Rtg-Tag-26

The routing tag of the route where Gateway-26 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.55 Gateway -27

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.56 Rtg-Tag-27

The routing tag of the route where Gateway-27 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.57 Gateway -28

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.58 Rtg-Tag-28

The routing tag of the route where Gateway-28 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.59 Gateway -29

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.60 Rtg-Tag-29

The routing tag of the route where Gateway-29 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.61 Gateway -30

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.62 Rtg-Tag-30

The routing tag of the route where Gateway-30 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.63 Gateway -31

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.64 Rtg-Tag-31

The routing tag of the route where Gateway-31 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.36.65 Gateway -32

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

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

2.2.36.66 Rtg-Tag-32

The routing tag of the route where Gateway-32 can be reached.

Console path:

Setup > **WAN** > **L2TP-Additional-Gateways**

Possible values:

0 … 65535

2.2.37 L2TP-Peers

In this table, the tunnel endpoints are linked with the L2TP remote stations that are used in the routing table. An entry in this table is required for outgoing connections if an incoming session should be assigned an idle timeout not equal to zero, or if the use of a particular tunnel is to be forced.

Console path:

Setup > **WAN**

2.2.37.1 Remote site

Name of the L2TP remote station.

Console path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

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

2.2.37.2 L2TP endpoint

Name of the tunnel endpoint

Console path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

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

2.2.37.3 SH time

Idle timeout in seconds.

Console path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

0 … 9999

2.2.37.5 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

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

Default:

DEFAULT

2.2.38 L2TP source check

The default setting checks the sender address of an incoming tunnel. The tunnel is established if the address is part of the configured gateway for the tunnel or if no gateways have been configured at all. It is also possible to check the routing tag of incoming packets. Note that only routing tags not equal to zero will be checked.

Console path:

Setup > **WAN**

Possible values:

Address
Tag+address

Default:

Address

2.2.39 L2TP-Ethernet

This table is used to link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.

Console path:

Setup > **WAN**

2.2.39.1 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 > **WAN** > **L2TP-Ethernet**

Possible values:

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

2.2.39.2 L2TP endpoint

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

Possible values:

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

2.2.39.3 Interface

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

Console path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtual L2TP Ethernet interfaces

2.2.40 DS-Lite-Tunnel

Dual-Stack Lite, abbreviated DS-Lite, is used so that Internet providers can supply their customers with access to IPv4 servers over an IPv6 connection. That is necessary, for example, if an Internet provider is forced to supply its customer with an IPv6 address due to the limited availability of IPv4 addresses. In contrast to the other three IPv6 tunnel methods "6in4", "6rd" and "6to4", DS-Lite is also used to transmit IPv4 packets on an IPv6 connection (IPv4 viaIPv6 tunnel).

For this, the device packages the IPv4 packets in an IPv4-in-IPv6 tunnel and transmits them unmasked to the provider, who then performs a NAT with one of their own remaining IPv4 addresses.

To define a DS-Lite tunnel, all the device needs is the IPv6 address of the tunnel endpoint and the routing tag with which it can reach this address.

Console path:

Setup > **WAN**

2.2.40.1 Name

Enter the name for the tunnel.

Console path:

Setup > **WAN** > **DS-Lite-Tunnel**

Possible values:

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

Default:

empty

2.2.40.2 Gateway address

This entry defines the address of the DS-Lite gateway, the so-called Address Family Transition Router (AFTR). Enter a valid value from the following selection:

- One IPv6 address (e.g. 2001:db8::1)
- An FQDN (Fully Qualified Domain Name) that can be resolved by DNS, e.g., aftr.example.com
- The IPv6 unspecified address "::" determines that the device should retrieve the address of the AFTRs via DHCPv6 (factory setting).
- An empty field behaves the same as the entry "::".

Console path:

Setup > **WAN** > **DS-Lite-Tunnel**

Possible values:

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

Default:

empty

2.2.40.3 Rtg-Tag

Enter the routing tag where the device reaches the gateway.

Console path:

Setup > **WAN** > **DS-Lite-Tunnel**

Possible values:

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

Default:

empty

2.2.40.5 Target-Interface

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

Console path:

Setup > **WAN** > **DS-Lite-Tunnel**

Possible values:

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

2.2.50 EoGRE-Tunnel

The current version of LCOS provides a number of "Ethernet over GRE" tunnels (EoGRE) to transmit Ethernet packets via GRE. You configure the various EoGRE tunnels here.

Console path:

Setup > **WAN**

2.2.50.1 Interface

Name of the selected EoGRE tunnel.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

2.2.50.2 Operating

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.50.3 IP address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

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

Default:

empty

2.2.50.4 Routing-Tag

Routing tag for the connection to the EoGRE tunnel endpoint.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

0 … 65535

Default:

0

2.2.50.5 Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.50.6 Key value

The key that assures data-flow control in this EoGRE tunnel.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

0 … 4294967295

Default:

0

2.2.50.7 Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.50.8 Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.50.9 Loopback address

This entry contains the loopback address of the EoGRE tunnel.

Console path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.2.51 GRE-Tunnel

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. You configure the various GRE tunnels here.

Console path:

Setup > **WAN**

2.2.51.1 Remote site

The name of the remote station for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

Console path:

Setup > **WAN** > **GRE-Tunnel**

2.2.51.3 IP address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

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

Default:

empty

2.2.51.4 Routing-Tag

Routing tag for the connection to the GRE tunnel endpoint.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

0 … 65535

Default:

0

2.2.51.5 Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.51.6 Key value

The key that assures data-flow control in this GRE tunnel.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

0 … 4294967295

Default:

0

2.2.51.7 Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.51.8 Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

2.2.51.9 Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.

If the list of IP networks or loopback addresses contains an entry named 'DMZ', then the associated IP address will be used.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Valid entry from the list of possible addresses.

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ

LB0 to LBF for the 16 loopback addresses

Any valid IP address

empty

Default:

2.2.51.11 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

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

Default:

DEFAULT

2.2.53 SSL-for-Action-Table

This menu contains the SSL settings for the action table.

Console path:

Setup > **WAN**

2.2.53.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.2.53.2 Key-exchange algorithms

Here you select the algorithms to be used for the key exchange.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.2.53.3 Crypto-Algorithms

Here you select the encryption algorithms to be used.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.2.53.4 Hash algorithms

Here you select the hash algorithms to be used.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

MD5
SHA1
SHA-256
SHA-384
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA-256

SHA-384

SHA2-256

SHA2-384

2.2.53.5 Prefer PFS

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

To disable this function, uncheck the box.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

Yes

Default:

Yes

2.2.53.6 Renegotiations

Specify whether new negotiations are permitted for secure connections.

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

No
Forbidden
Allowed
Ignored

Default:

Allowed

2.2.53.7 Elliptic curves

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

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

2.2.53.21 Signature hash algorithms

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

Console path:

Setup > **WAN** > **SSL-for-Action-Table**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.2.60 VLANs

This menu contains the editable configuration of VLAN assignments for different Internet service providers.

Console path:

Setup > **WAN**

2.2.60.1 Provider list

This table contains the Internet service providers for whom VLANs should be checked in addition to VLAN 0. For this check, LCOS uses the "User name" entry in the PPP list under **Communication** > **Protocols**.

Console path:

Setup > **WAN** > **VLANs**

2.2.60.1.1 Providers

Here you enter the user name specified under **Communication** > **Protocols** > **PPP list** in order to identify Internet service providers that require the checking of additional VLANs.

"*" is defined as a wild card for this field so that, for example, entering "`*@t-online.de`" causes the setting to be applied to all PPP list entries that end with @t-online.de.

Console path:

Setup > **WAN** > **VLANs** > **Provider-List**

Possible values:

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

Default:

empty

2.2.60.1.2 VLAN-IDs

Here you specify the VLANs that are to be checked in addition to VLAN 0. The checking of additional VLANs only takes place if the entry under *2.2.60.1.1 Providers* on page 148 matches the user name in the PPP list.

You have the option of specifying a single VLAN or multiple comma-separated VLANs.

Console path:

Setup > **WAN** > **VLANs** > **Provider-List**

Possible values:

Max. 64 characters from `[0-9]-,`

Default:

empty

2.2.62 Provider-Specifics

Some providers transmit the actual available layer-3 bandwidth after a successful PPP login (PPP PAP-ACK). This is relevant if the synchronized DSL bandwidth differs from the bandwidth agreed in the Internet tariff or if the actual bandwidth is unknown, such as with fiber-optic or Ethernet-based connections. In this case, the least value of the transmitted bandwidth and the DSL information is used as the QoS value. This information helps to operate of Quality of Service effectively.

This table contains login IDs with wildcards, for example to extract the actual up- and downstream speeds from the PAP ACK message sent during login.

If the table does not contain a matching login ID, then all of the parameter strings defined in the table are checked for a match. The first hit is taken and the up-/download rates are applied accordingly.

These values are displayed in the status menu under **Status** > **WAN** > **Connection-Bandwidth**. It shows the bandwidth synchronized by DSL, the bandwidth transmitted by the provider, as well as the resulting bandwidth used by the QoS.

Console path:

Setup > **WAN**

2.2.62.1 Provider

Provider login ID; may contain wildcards.

Console path:

Setup > **WAN** > **Provider-Specifics**

Possible values:

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

Default:

empty

2.2.62.2 Parameter-Format

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

- {txrate} – Upstream-Rate
- {rxrate} – Downstream-Rate

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

Console path:

Setup > **WAN** > **Provider-Specifics**

Possible values:

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

Default:

empty

2.2.63 464XLAT

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

Console path:

Setup > **WAN**

2.2.63.1 Peer

Set a unique name for this peer.

Console path:

Setup > **WAN** > **464XLAT**

Possible values:

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

2.2.63.2 Target-Interface

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

Console path:

Setup > **WAN** > **464XLAT**

Possible values:

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

2.2.63.3 Subnet-ID

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

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

Console path:

Setup > **WAN** > **464XLAT**

Possible values:

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

Default:

empty

2.2.63.4 PLAT-Prefix

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

Console path:

Setup > **WAN** > **464XLAT**

Possible values:

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

Default:

64:ff9b::/96

2.2.63.6 CLAT-Mode

Defines with which method the CLAT prefix should be generated.

Console path:

Setup > **WAN** > **464XLAT**

Possible values:

DHCPv6-PD

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

WWAN

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

Static

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

Default:

WWAN

2.2.64 Manual-Action-Start

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

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

The result of the execution can be analyzed with the “connact” trace.

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

Console path:

Setup > **WAN**

Possible arguments:

[-4 <IPv4-address>]

Optional specification of an IPv4 address

[-6 <IPv6-address>]

Optional specification of an IPv6 address

<Connection-Name>[/<Condition>]

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

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

2.2.71 QoS

LCOS supports up to eight different queues (service classes) with corresponding priority levels for applications in the network, and include "VoIP", "Gold", "Silver" or "Best Effort". Data packets are assigned to the appropriate Quality of Service (QoS) class using DSCP markings or firewall rules. The router then sorts the packets into the correct priority level and ensures that the corresponding services only use as much upload bandwidth as was previously configured for the class in percent or Mbps. This ensures that important services such as VoIP or video calls always receive sufficient bandwidth, even when the network is under heavy load.

In the following explains the concept of how Quality of Service functions with eight queues. Routers should fundamentally be able to prioritize packets according to the DSCP value in the IP header. A total of eight **queues** are available for this purpose, which are strictly prioritized. This means that packets are sent starting with the **queue** with the highest priority and working through to the **queue** with the lowest priority. A packet is assigned to a **queue** based either on the DSCP value in the IP header or by a firewall rule. Of the eight available **queues** two are reserved, one for the **Urgent-Queue** (highest priority, for internal services such as VCM and protocol packets) and the other for the **Best-Effort-Queue** (lowest priority, for all non-priority packets). The remaining six **queues** are freely available to the user. The priority levels of the individual **queues** are set by placing them in a **Queue-List** in descending order of priority. The internal **Urgent-Queue** and **Best-Effort-Queue** are inserted at the front and end of this **Queue-List**. The completed **queue list** must then be assigned to a physical **WAN interface**. Following this, any packets sent to this **WAN interface** are prioritized according to the configuration of the **queues**.

For QoS to work, the bandwidths or rates of an interface must be known in order for QoS to correctly distribute the load, e.g. in the case where bandwidths are allocated as a percentage. The bandwidths are usually taken from the upstream and downstream data rates from the internal DSL modems or from the bandwidth transmitted in the PPP by the provider.

Console path:

Setup > **WAN**

2.2.71.1 Congestion-Action

The Congestion Action determines how a backed-up send queue is handled. Since this queue cannot grow indefinitely, packets must be discarded at some point. Two mechanisms are available here: **Taildrop** and **Random Early Detection (RED)** , also known as **Random Early Discard**. With taildrop, a limit is set beyond which all further incoming packets are discarded. In RED, two limits are determined. As of the first one, packets are discarded with a probability P. P increases the closer you get to the second limit. If the second limit is exceeded, all incoming packets are discarded, like taildrop.

The table **Congestion-Action** is defined in such a way that it can be configured to contain **RED** and **Taildrop**. This decision ensures maximum flexibility, on the one hand, but also a high potential for errors leading to a non-functional configuration. Hence the following explanation of the framework conditions for both concepts. A **Taildrop** is recognized by the fact that **Threshold-Min** is equal to **Threshold-Max**. **Max-Probability** with

a **Taildrop** has no purpose, but should be entered as 100 to indicate that everything above the limit will be discarded. For a user to configure a **Taildrop** as easily as possible, a shortened input can be used:

```
root@:/Setup/WAN/QoS
> add Congestion-Action/test bytes 2000
set ok:
Name                 Metric-Type   Threshold-Min    Threshold-Max    Max-Probability-Percentage
====================-------------------------------------------------------------------------
TEST                 Bytes         2000             2000             100
```

You only specify the **Metric-Type** and **Limit-Min**, the other values are set so that a **Taildrop** is configured.

For a **RED**, the **Threshold-Min** is not equal to **Threshold-Max**. The packet is discarded as of **Threshold-Min** starting with a probability P=0, where P linearly approaches **Max-Probability** the closer you get to **Threshold-Max**.

Console path:

Setup > **WAN** > **QoS**

2.2.71.1.1 Name

The name of the **Congestion-Action** entered here is used to reference the entry from other tables. The name must be unique within this table.

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$&'()+-,/:;<=>?[\]^_.`

2.2.71.1.2 Metric-Type

This specifies which metric is used by the values in columns *2.2.71.1.3 Threshold-Min* on page 153 and *2.2.71.1.4 Threshold-Max* on page 154

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

Frames
Bytes
KBytes

2.2.71.1.3 Threshold-Min

Specifies the lower threshold for the **Congestion-Action**.

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

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

2.2.71.1.4 Threshold-Max

Specifies the upper threshold for the **Congestion-Action**. From here on, all packets are discarded.

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

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

2.2.71.1.5 Max-Probability-Percentage

Specifies the maximum drop probability for a configured **RED**. Is ignored if there is a **Taildrop** and should be set to 100 there.

Console path:

Setup > **WAN** > **QoS** > **Congestion-Action**

Possible values:

0 … 100

2.2.71.2 Queues

This table is used to configure **queue templates**. This does not mean that every entry in this table creates a queue. A **queue** is only created when it is used in a **Queue-List** and assigned to a **WAN interface**. This means a template created here can be the basis for any number of **queues** or none at all.

Example: If an entry named "Test" is created and this entry is then divided into two **Queue-List** objects, each of which is assigned to a different **WAN interface**, then the result will be two **queues** with name "Test", which are completely independent of one another.

Console path:

Setup > **WAN** > **QoS**

2.2.71.2.1 Name

This is where the name of the **queue template** is entered. Other tables reference the template by using this name. The name must be unique within the table.

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$&'()+-,/:;<=>?[\]^_.`

2.2.71.2.2 Metric-Type

This is where the metric of the columns *2.2.71.2.3 Commit-Rate* on page 155 and *2.2.71.2.4 Excess-Rate* on page 155 is set.

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Percentage

The rate is given as a percentage. The basic value for the calculation is the bandwidth available on the WAN interface.

Kbit

The rate is nominally given in kilobits per second.

Mbit

The rate is nominally given in megabits per second.

2.2.71.2.3 Commit-Rate

Here you enter how much bandwidth is available to this **Queue**. The value is also commonly referred to as CIR (Committed Information Rate). The unit of the input is set in the column *2.2.71.2.2 Metric-Type* on page 155. The following value ranges apply:

- *Percent:* 1 < x < 100
- *Kbit:* 1 < x < 4294967295
- *Mbit:* 1 < x < 4294967295

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

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

2.2.71.2.4 Excess-Rate

Here you enter the bandwidth the **Queue** can use in addition to its **Commit-Rate**. The value is also commonly referred to as EIR (Excess Information Rate). To prevent higher-priority **queues** from taking the **commit rate** of lower-priority **queues**, the following concept was used:

The QoS operates in time slots, during which each **queue** can use its **commit rate**. At the end of the time slot, the unused **Commit-Rate** from all **queues** is carried over into the next time slot and used as a pool for the **Excess-Rate**. This pool then limits the bandwidth that can be used with the **Excess-Rate**. This fulfills two important aspects: Firstly, the **Excess-Rate** of a queue is not subtracted from another queue's current **Commit-Rate**, but from the unused rate of the previous time slot. Second, the pool for the **Excess-Rate** is reset at the beginning of each time slot and is not added up, which means the unused **Commit-Rate** of a time slot can only be used in the following time slot. This prevents an accumulation, which could cause **queues** with a configured excess rate to starve the lower-priority queues.

Example: Two **queues** are configured, concatenated into a **Queue-List**, and assigned to a **WAN interface**. **Queue A** has a **commit rate** of 10 Mbps and an **excess rate** of 4 Mbps. **Queue B** has a **commit rate** of 5 Mbps and an **excess rate** of 0. If now in time slot 1 **Queue A** uses 9 Mbps and **Queue B** uses 4 Mbps, then 2 Mbps are unused rate and added to the pool of the **excess rate** for time slot 2. In this time slot, **Queue A** can then use its 10 Mbps **commit rate**

and an additional 2 Mbps from the pool as part of its **excess rate**. Important is that only as much **Excess-Rate** can be used as the pool provides.

The unit of the input is set in the column *2.2.71.2.2 Metric-Type* on page 155. The following value ranges apply:

- *Percent:* 0 < x < 100
- *Kbit:* 0 < x < 4294967295
- *Mbit:* 0 < x < 4294967295

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

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

2.2.71.2.5 Fallback-to-Best-Effort

This control determines what happens to packets that cannot be sent as part of the commit rate or excess rate.

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

Yes

The packets are sent via the best-effort queue.

No

The packets are discarded.

2.2.71.2.6 Congestion-Action

This references an object from the table *2.2.71.1 Congestion-Action* on page 152, which determines when packets are discarded due to full send queues.

Console path:

Setup > **WAN** > **QoS** > **Queues**

2.2.71.2.7 DSCP-Tags

The DSCP tags (Differentiated Services Code Point) to be assigned to this queue are entered here. Multiple values can be passed using a comma-separated list.

Console path:

Setup > **WAN** > **QoS** > **Queues**

Possible values:

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

2.2.71.3 Queue-List

The configured **queue templates** are concatenated into a **queue list** here. This is done by a comma-separated list, with the order specifying the priority from high to low.

It is when creating a **queue list**, make sure that the **commit rates** of the **queues** do not overbook the bandwidth of the **WAN interface**. Otherwise, the low priority **queues** may be starved.

It is also important to ensure that **DSCP tags** are not assigned multiple times. If this happens, the nature of the implementation means that the tag is assigned to the lowest-priority **queue**.

Console path:

Setup > **WAN** > **QoS**

2.2.71.3.1 Name

This name is used to reference the **Queue-List** from other tables. It must be unique within the table.

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$&'()+-,/:;<=>?[\]^_.`

2.2.71.3.2 Best-Effort-Congestion-Action

This references a **Congestion-Action** in the Congestion-Action table to assign a **Congestion-Action** to the **Best-Effort-Queue**. By default, the DEFAULT entry is used.

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

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

2.2.71.3.3 Ordered-List

A comma-separated list of **queue templates** is entered here, with their priorities ranging from high to low. Up to six of your own custom **queue templates** be concatenated here, since two places are reserved for the internal **Urgent-Queue** and **Best-Effort-Queue**.

Example of a list: Gold, silver, bronze. The priority of the queues starts with gold, then silver and bronze.

Console path:

Setup > **WAN** > **QoS** > **Queue-List**

Possible values:

Max. 120 characters from `[A-Z][0-9]@{|}~!$&'()+-,/:;<=>?[\]^_.`

2.2.71.4 Interfaces

Configured **queue lists** are assigned to **WAN interfaces** here.

Console path:

Setup > **WAN** > **QoS**

2.2.71.4.1 Interface

Enter the name of the physical **WAN interface** here. Entries are limited to the **WAN interfaces** available on the device.

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

2.2.71.4.2 Enabled

This switches the configured QoS on the **WAN interface** on or off.

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

Yes
No

2.2.71.4.3 Queue-List

This references an entry in the queue-list table.

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$&'()+-,/:;<=>?[\]^_.`

2.2.71.4.4 Maximum-Burst-Size

The Maximum Burst Size (MBS) regulates the number of bytes that can be sent within a short period (burst). This parameter ensures that massively or continuously oversubscribed traffic does not completely exhaust the available buffer resources, e.g., on upstream provider routers. The value should be set according to the provider's specifications for the subscribed connection.

Console path:

Setup > **WAN** > **QoS** > **Interfaces**

Possible values:

max. 5 characters `[0-9]`

Default:

0

Special values:

0

The default value 0 means that the operating system manages the parameter internally. Typically, the internal value corresponds to the MTU of the used WAN connection.

2.3 Charges

This menu contains the settings for charge management.

Console path:

Setup

2.3.2 Days-per-Period

Specify a period in days that will serve as the basis for the controlling the charges and time limits.

Console path:

Setup > **Charges**

Possible values:

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

Default:

1

2.3.7 Time-Table

This table displays an overview of configured budgets for your interfaces, sorted by budget minutes.

Console path:

Setup > **Charges**

2.3.7.1 Ifc.

The interface referred to by the entry.

Console path:

Setup > **Charges** > **Time-Table**

2.3.7.2 Budget-minutes

Displays the budgeted minutes used up for this interface.

Console path:

Setup > **Charges** > **Time-Table**

2.3.7.3 Spare-Minutes

Displays the remaining budgeted minutes for this interface.

Console path:

Setup > **Charges** > **Time-Table**

2.3.7.4 Minutes-active

Displays the budgeted minutes of activity for data connections on this interface.

Console path:

Setup > **Charges** > **Time-Table**

2.3.7.5 Minutes-passive

Displays the budgeted minutes that this interface was connected passively.

Console path:

Setup > **Charges** > **Time-Table**

2.3.8 DSL-Broadband-Minutes-Budget

Specify here the maximum number of online minutes that can be consumed in the time period defined above. Once this limit is reached, the device establishes no further connections.

Console path:

Setup > **Charges**

Possible values:

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

Default:

600

2.3.9 Spare-DSL-Broadband-Minutes

Displays the number of minutes remaining for DSL broadband connections in the current period.

Console path:

Setup > **Charges**

2.3.10 Router-DSL-Broadband-Budget

Displays the number of minutes used by DSL broadband connections in the current time period.

Console path:

Setup > **Charges**

2.3.11 Reserve-DSL-Broadband-Budget

Specify here the number of additional online minutes that are permitted within the above time period if the reserve is activated.

Console path:

Setup > **Charges**

Possible values:

max. 10 characters from `[0–9]`

Default:

300

2.3.12 Activate-Additional-Budget

You can manually reset units, time and volume budgets.

Enter the name of the WAN connection as the parameter. You can reset all volume budgets with the parameter "*". If you do not specify a parameter, you reset only the unit- and time counters.

By resetting the current budget, you remove any charge limiter that may be in effect.

Console path:

Setup > **Charges**

2.3.14 Spare-Dialup-Minutes

Displays the number of minutes remaining for dial-in connections in the current period.

Console path:

Setup > **Charges**

Possible values:

max. 10 characters from `[0–9]`

Default:

210

2.3.16 Reset-Budgets

Some providers allow you an additional data volume or time limit if your budget is reached. This action can be used to increase the volume- or time budget by an appropriate amount.

Specify the name of the WAN connection as well as the amount of the budget in MB as additional parameters. If you do not specify a budget, you approve the full amount of the budget specified for this WAN connection.

By activating an additional budget, you remove any charge limiter that may be in effect.

Console path:

Setup > **Charges**

2.3.17 Volume-Budgets

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. In this directory, you can set a data volume for each connection/remote station and define an action that the device should perform when this limit is exceeded.

Console path:

Setup > **Charges**

2.3.17.1 Peer

Name of the remote station for which this data volume applies.

Select from the list of defined peers.

Console path:

Setup > **Charges** > **Volume-Budgets**

Possible values:

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

Default:

empty

2.3.17.2 Limit-MB

Data volume in megabytes that applies to the specified remote station.

Console path:

Setup > **Charges** > **Volume-Budgets**

Possible values:

0 … 4294967295 MBytes

Default:

0

Special values:

0

No monitoring of data volume.

2.3.17.3 Action

Action to be executed by the device when the budget is exceeded.

You can also specify that the device should perform multiple actions. If they include the action **disconnect**, the device performs this action as the last one.

Console path:

Setup > **Charges** > **Volume-Budgets**

Possible values:

syslog

The device stores a SYSLOG message (with the flag "Critical") that you can analyze with LANmonitor or a special SYSLOG client.

mail

The device sends a message to the e-mail address that you specified under **Setup** > **Charges** > **Charging-Email**.

disconnect

The device disconnects from the remote station.

The **disconnect** action activates the charge limiter. The device can no longer connect to this remote until the end of the month unless you increase the volume budget for this remote site.

2.3.18 Free networks

If data transfer to certain networks does not affect the volume budget for a remote site, you can exclude these networks from the budgeting.

Console path:

Setup > **Charges**

2.3.18.1 Peer

Name of the remote station for which this exception applies. Select from the list of defined peers.

You can make multiple entries for each remote by suffixing the name of the remote station with the # character and adding a number (e.g. "INTERNET", "INTERNET#1", "INTERNET#2", etc.). This is useful if you explicitly wish to define an exception that is only temporarily active. When this exception is no longer valid, you delete only the entry with the correspondingly numbered remote station.

Console path:

Setup > **Charges** > **Free-Networks**

Possible values:

max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.3.18.2 Free networks

Using this parameter, you can define individual IPv4 and IPv6 addresses as well as entire networks (for example by using the prefix notation "192.168.1.0/24"), which are excluded from the budget monitoring.

Multiple values can be specified in a comma-separated list.

Console path:

Setup > **Charges** > **Free-Networks**

Possible values:

max. 100 characters from `[0-9]/.`

Default:

empty

2.3.19 Budget-Control

In this directory you specify when the device starts recording the budget each month.

Console path:

Setup > **Charges**

2.3.19.1 Peer

Name of the remote station for which this time applies. Select from the list of defined peers.

You can use wildcards for the names of the remote stations. The wild card "*" in this case applies for all remote stations.

Console path:

Setup > **Charges** > **Budget-Control**

Possible values:

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

Default:

empty

2.3.19.2 Day

Day of the month when the device resets the monthly data-volume budget monitoring.

Console path:

Setup > **Charges** > **Budget-Control**

Possible values:

1 … 31

Default:

1

2.3.19.3 Hour

Hour when the device resets the data-volume budget monitoring.

Console path:

Setup > **Charges** > **Budget-Control**

Possible values:

0 … 23

Default:

0

2.3.19.4 Minute

Minute when the device resets the data-volume budget monitoring.

Console path:

Setup > **Charges** > **Budget-Control**

Possible values:

0 … 59

Default:

0

2.3.20 Charging-Email

If the device should send an e-mail when the volume of data is exceeded, specify the valid e-mail address here.

Console path:

Setup > **Charges**

Possible values:

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

Default:

empty

2.4 LAN

If the device should send an e-mail when the volume of data is exceeded, specify the valid e-mail address here.

Console path:

Setup

2.4.2 MAC-Address

This is the hardware address of the network adapter in your device.

Console path:

Setup > **LAN**

2.4.3 Heap-Reserve

The spare-heap value indicates how many blocks of the LAN heap are reserved for communication with the device over HTTP(S)/Telnet(S)/SSH. This heap is used to maintain the device's accessibility even in case of maximum load (or if queue blocks get lost). If the number of blocks in the heap falls below the specified value, received packets are dropped immediately (except for TCP packets sent directly to the device).

Console path:

Setup > **LAN**

Possible values:

0 … 999

Default:

10

2.4.8 Trace-MAC

Use this value to limit the Ethernet trace to those packets that have the specified MAC address as their source or destination address.

Console path:

Setup > **LAN**

Possible values:

max. 16 characters from `[A-F][a-f][0-9]`

Default:

000000000000

Special values:

000000000000

If set to 000000000000, the Ethernet trace outputs all packets.

2.4.9 Trace-Level

The output of trace messages for the LAN-Data-Trace can be restricted to contain certain content only.

Console path:

Setup > **LAN**

Possible values:

0 … 255

Default:

255

Special values:

0

Reports that a packet has been received/sent.

1

Additionally the physical parameters of the packet (data rate, signal strength…)

2

Adds the MAC header

3

Adds the Layer-3 header (e.g. IP/IPX)

4

Adds the Layer-4 header (TCP, UDP…)

5

Additionally the TCP/UDP payload

255

Output is not limited

2.4.10 IEEE802.1x

This menu contains the settings for the integrated 802.1x supplicant. The device requires these settings, for example, if it is connected to an Ethernet switch with activated 802.1x authentication.

Console path:

Setup > **LAN**

2.4.10.1 Supplicant-Ifc-Setup

This table controls the function of the integrated 802.1x supplicant for the available LAN interfaces.

Console path:

Setup > **LAN** > **IEEE802.1x**

2.4.10.1.1 Ifc

Here you select the LAN interface that the settings for the 802.1x supplicant apply to. Choose from the LAN interfaces available in the device, e.g. LAN-1 or LAN-2.

Console path:

Setup > **LAN** > **IEEE802.1x** > **Supplicant-Ifc-Setup**

2.4.10.1.2 Method

Here you select the method to be used by the 802.1x supplicant for authentication.

Console path:

Setup > **LAN** > **IEEE802.1x** > **Supplicant-Ifc-Setup**

Possible values:

None
The value "None" disables the 802.1x supplicant for the respective interface.
MD5
TLS
TTLS/PAP>
TTLS/CHAP
TTLS/MSCHAP
TTLS/MSCHAPv2
TTLS/MD5
PEAP/MSCHAPv2
PEAP/GTC

Default:

None

2.4.10.1.3 Credentials

Depending on the EAP/802.1X method, enter the credentials necessary to login. TLS requires nothing to be entered here. The authentication is carried out with the EAP/TLS certificate stored in the file system. For all other methods, enter the user name and password in the format "user:password".

Console path:

Setup > **LAN** > **IEEE802.1x** > **Supplicant-Ifc-Setup**

Possible values:

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

Default:

empty

2.4.10.3 Authenticator-Ifc-Setup

This menu contains the settings for the RADIUS authentication (802.1X authentication) of clients connecting to the device via the LAN interfaces.

Console path:

Setup > **LAN** > **IEEE802.1X**

2.4.10.3.1 Ifc

Name of the port.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

2.4.10.3.2 Operating

Use this parameter to specify whether 802.1X authentication is required for this port.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Possible values:

No
Yes

Default:

No

2.4.10.3.3 Mode

This item sets whether one or more clients may login at this interface via IEEE 802.1X.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Possible values:

Single host

Just one client can authenticate and then operate on this port. If a further client with its own MAC address is detected on this port, the port is reset to the unauthenticated state.

Multiple host

Several clients (with different MAC addresses) can operate on this port. Authentication only needs to be performed once. This mode can be used, for example, if a WLAN access point is operated on a port configured in this way and the payload data is not tunneled to a central controller. In this case, data packets from WLAN clients that have their own MAC addresses would also be seen on the Ethernet port configured in this way.

Multiple auth

Several clients can each perform their own 802.1X authentication on this port.

Default:

Single host

2.4.10.3.4 RADIUS-Server

Specifies which RADIUS server is used both for 802.1X and for MAC address validation. To do this, reference one of the entries under *2.30.3 RADIUS server* on page 1039 or create a new entry there if necessary. You can adjust the format of the transmitted MAC address under *2.4.10.4 Username-Attribute-Format* on page 172.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Possible values:

Name from **Setup** > **IEEE802.1X** > **RADIUS-Server**

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

2.4.10.3.5 MAC-Auth.-Bypass

This specifies whether a failed attempt to start an 802.1X negotiation should be followed by a check of the client's MAC address via RADIUS and a subsequent opening of the port. In this case, the MAC address is transmitted as a RADIUS user name and password in the format "aabbccddeeff". It must also be stored in the RADIUS server in this format.

The MAC address is easy to fake and does not protect against malicious attacks.

In the standard configuration, the 802.1X authenticator will try to start an 802.1X negotiation for 90 seconds before falling back to the MAC address check. This time can be adjusted for each port by changing the parameters *2.30.4.5 Max-Req* on page 1043 (default: 3 attempts) and *2.30.4.7 Supp-Timeout* on page 1043 (default: 30 seconds). Alternatively, the mode for MAC Auth Bypass can be set to "Immediate". This mode immediately starts a MAC address check without waiting for a timeout.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Possible values:

No

MAC address authentication is not possible.

Yes

MAC address authentication is possible.

Immediate

Authentication is immediately performed by MAC address.

Default:

No

2.4.10.3.6 Bypass-RADIUS-Server

The RADIUS server specified here is used only for the MAC authentication bypass. This allows separate RADIUS servers to be used for 802.1X and the MAC authentication bypass. To do this, reference one of the entries under *2.30.3 RADIUS server* on page 1039 or create a new entry there if necessary. You can adjust the format of the transmitted MAC address under *2.4.10.4 Username-Attribute-Format* on page 172.

Console path:

Setup > **LAN** > **IEEE802.1X** > **Authenticator-Ifc-Setup**

Possible values:

Name from **Setup** > **IEEE802.1X** > **RADIUS-Server**

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

2.4.10.4 Username-Attribute-Format

The format of the MAC address that is transmitted to the RADIUS server during MAC authentication can be configured here.

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

Console path:

Setup > **LAN** > **IEEE802.1X**

Possible values:

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

Default:

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

2.4.11 Linkup-Report-Delay-ms

This setting specifies the time (in milliseconds) after which the LAN module signals to the device that a link is "up" and data transfer can begin.

Console path:

Setup > **LAN** > **IEEE802.1x**

Possible values:

0 … 4294967295

Default:

50

2.4.12 HNAT

With this setting you enable or disable the use of hardware NAT on the QVER platform. With HNAT enabled, the hardware can handle the routing WAN connection data, which increases the throughput and reduces the CPU load on your device.

HNAT is only available on devices of the 1781 series with an Ethernet switch AR8327N as well as the WLC4006+.

Console path:

Setup > **LAN** > **IEEE802.1x**

Possible values:

No
Yes

Default:

No

2.4.13.11.1 Interface bundling

This table contains the settings for bundling the physical and logical interfaces.

By bundling interfaces, it is possible to transmit data packets on two paired interfaces. To do this, the device duplicates outgoing data packets and transmits them on each of the two interfaces simultaneously. When receiving packets, the device accepts the first incoming packets; duplicates are detected and discarded by the device.

Using interface bundling makes it possible to reduce packet failure rates and latency times for data transmissions, although this does reduce the maximum bandwidth of the corresponding interface.

Console path:

Setup > **LAN**

2.4.13.1 Interfaces

This menu contains the settings for interface bundling.

Console path:

Setup > **LAN** > **Interface-Bundling**

2.4.13.1.1 Interface

This parameter indicates shows the logical cluster interface used for bundling the selected logical and physical interfaces of the devices.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

BUNDLE-1
BUNDLE-2

2.4.13.1.2 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 A and B that are selected in the corresponding table can still be used as individual interfaces.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

Yes
No

Default:

No

2.4.13.1.3 Protocol

Set the protocol that is used for interface bundling using these parameters.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

PRP
Sets the Parallel Redundancy Protocol (PRP).

2.4.13.1.4 MAC address

Using this parameter you can set an alternative MAC address for use by the corresponding bundle interface.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

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

Special values:

empty

If you leave this field empty, the device uses the system-wide MAC address.

Default:

Depends on the MAC address of your device

2.4.13.1.5 Interface-A

Using this parameter you select the 1st physical or logical link that this device bundles.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

Select from the available interfaces.

Default:

WLAN-1

2.4.13.1.6 Interface-B

Using this parameter you select the 2nd physical or logical link that this device bundles.

Console path:

Setup > **LAN** > **Interface-bundling** > **Interfaces**

Possible values:

Select from the available interfaces.

Default:

WLAN-2

2.4.13.12 LACP

This menu is used to configure the Link Aggregation Control Protocol (LACP).

Console path:

Setup > **LAN** > **Interface-Bundling**

2.4.13.12.1 Interfaces

Select an interface bundle here.

Console path:

Setup > **LAN** > **Interface-Bundling** > **LACP**

Possible values:

BUNDLE-1
Interface bundle 1
BUNDLE-2
Interface bundle 2

2.4.13.12.1.1 Interface

Use this menu to access the advanced features.

Console path:
Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

General
Contains previously known features of the interface bundling.
Advanced
Contains new features of the interface bundling.

Default:

General

2.4.13.12.1.2 System-Priority

Set the system priority here.

Console path:
Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:
Multiples of 4096 `[0-9]`

Default:
32768

2.4.13.12.1.3 Key

Here, you assign a number as an identifier for the bundle.

Console path:
Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:
1 … 54

Default:

42

2.4.13.12.1.4 Frame distribution policy

Outbound packets from the transmitting end are distributed to the individual interfaces within the link aggregation group (LAG) according to the frame distribution policy.

Console path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

VLAN

Outbound packets are distributed to the individual links of the LAG according to their VLAN tags.

Flow hash

For outbound packets, a flow hash is formed from the IP addresses and the TCP/UDP ports. The flow hash determines how the packets are distributed to the individual links of the LAG.

Source MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address.

Destination MAC

Outbound packets are distributed to the individual links of the LAG according to their destination MAC address.

Source-dest. MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address and destination MAC address.

Default:

Flow hash

2.4.13.12.1.5 Port priority A

Here you set the status values for port priority A.

Console path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

Multiples of 4096 `[0-9]`

Default:

32768

2.4.13.12.1.6 Port priority B

Here you set the status values for port priority A.

Console path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

Multiples of 4096 `[0-9]`

Default:

32768

2.7 TCP-IP

This menu contains the TCP/IP settings.

Console path:

Setup > **LAN**

2.7.1 Operating

Activates or deactivates the TCP-IP module.

Console path:

Setup > **LAN** > **TCP-IP**

Possible values:

no
yes

Default:

yes

2.7.6 Access-List

The access list contains those stations that are to be granted access to the device's configuration. If the table contains no entries, all stations can access the device.

Console path:

Setup > **LAN** > **TCP-IP**

2.7.6.1 IP-Address

Valid IP address of the station that is to be granted access to the device's configuration.

Console path:

Setup > **LAN** > **TCP-IP** > **Access-List**

2.7.6.2 IP-Netmask

Valid IP netmask of the station that is to be given access to the device's configuration.

Console path:

Setup > **LAN** > **TCP-IP** > **Access-List**

2.7.6.3 Rtg-Tag

Routing tag for selecting a specified route.

Console path:

Setup > **LAN** > **TCP-IP** > **Access-List**

Possible values:

max. 16 characters from `[0-9]`

Default:

empty

2.7.6.4 Comment

This parameter allows you to enter a comment on the entry.

Console path:

Setup > **TCP-IP** > **Access-List**

Possible values:

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

Default:

empty

2.7.7 DNS-Default

Specify here the address of a name server to which DNS requests are to be forwarded. This field can be left empty if you have an Internet provider or other remote site that automatically assigns a name server to the device when it logs in.

Console path:

Setup > **LAN** > **TCP-IP**

Possible values:

max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.7.8 DNS-Backup

Specify here a name server to be used in case the first DNS server fails.

Console path:

Setup > **LAN** > **TCP-IP**

Possible values:

max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.7.11 ARP-Aging-Minutes

Here you can specify the time in minutes after which the ARP table is updated automatically, i.e. any addresses that have not been contacted since the last update are removed from the list.

Console path:

Setup > **LAN** > **TCP-IP**

Possible values:

1 … 60 minutes

Default:

15

2.7.16 ARP-Table

The address resolution protocol (ARP) determines the MAC address for a particular IP address and stores this information in the ARP table.

Console path:

Setup > **LAN** > **TCP-IP**

2.7.16.1 IP-Address

Valid IP address for which a MAC address was determined.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.2 MAC-Address

MAC address matching the IP address in this entry.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.3 Last-access

The time when this station last access the network.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.5 Ethernet-Port

Physical interface connecting the station to the device.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.6 Peer

Select the remote device over which the station can be reached from the list of defined peers.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.7 VLAN-ID

VLAN ID of network where the station is located.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.16.8 Connector

Logical interface connecting the device.

Console path:

Setup > **LAN** > **TCP-IP** > **ARP-Table**

2.7.17 Loopback-List

This table is used to configure alternative addresses.

Console path:

Setup > **LAN** > **TCP-IP**

2.7.17 Loopback-Addr.

You can optionally configure up to 16 loopback addresses here. The device considers each of these addresses to be its own address and behaves as if it has received the packet from the LAN. This applies in particular to masked connections. Answers to packets sent to a loopback address are not masked.

Console path:

Setup > **LAN** > **TCP-IP** > **Loopback-List**

Possible values:

Name of the IP networks whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.

2.7.17.2 Name

You can enter a name with a max. 16 characters here.

Console path:

Setup > **LAN** > **TCP-IP** > **Loopback-List**

Possible values:

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

Default:

empty

2.7.17.3 Rtg tag

Here you specify the routing tag that identifies routes to remote gateways that are not configured with their own routing tag (i.e. the routing tag is 0).

Console path:

Setup > **TCP-IP** > **Loopback-List**

Possible values:

0 … 65,535

Default:

0

2.7.20 Non-Loc.-ARP-Replies

When this option is activate the device will reply to ARP requests for its address even if the sender address is not located in its own local network.

Console path:

Setup > **TCP-IP**

2.7.21 Alive-Test

This menu contains the settings for the alive test. The alive test sends a ping to a destination address at configurable intervals. If the destination does not respond, the device performs a reboot or other action according to defined criteria.

To configure the alive test you have to define the target address, the action to be performed, the combination of pings and retries, and the threshold for triggering the defined action. The parameters required for this have the following default values:

Fail-Limit

Default value: 10

Test Interval:

Default value: 10

Retry-Interval

Default value: 1

Retry-Count

Default value: 1

These settings cause the device to transmit a ping every 10 seconds (test interval). If this ping is not answered, the device repeats the ping after 1 second (retry interval) and exactly one time (retry count). If this ping also goes unanswered, the device considers the series to have failed. If 10 series in a row fail (fail limit) then the device triggers the defined action, in this case after 10 x 10 seconds = 100 seconds.

Console path:

Setup > **TCP-IP**

2.7.21.1 Target-Address

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

Max. 15 characters from `[0-9].`

2.7.21.2 Test Interval:

The time interval in seconds, in which the device sends a ping to the target address. If the ping is unanswered, the device optionally repeats a set number of pings in the defined interval. With this configuration, the device forms a "series" of ping attempts. Only when all pings go unanswered is the complete series evaluated as unsuccessful.

The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

Select the test interval as a time which is greater than the product of the retry interval and retry count, so that the desired number of retries can be performed within the test interval.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

0 … 4294967295 Seconds

Default:

10

2.7.21.3 Retry-Count

If a ping goes unanswered, this value defines the number of times that the device will repeat the ping to the target address.

Set the retry count to a number such that the product of retry interval and retry count is less than the test interval. This ensures that the desired number of retries can be performed within the test interval.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

0 … 4294967295 Seconds

Default:

1

Special values:

0

With a retry count of 0 the device sends no repeat pings.

2.7.21.4 Retry-Interval

If a ping goes unanswered, this value defines the time interval before the device repeats the ping to the target address.

Set the retry interval to a number such that the product of retry interval and retry count is less than the test interval. This ensures that the desired number of retries can be performed within the test interval.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

0 … 4294967295 Seconds

Default:

1

Special values:

0

With a retry interval of 0 the device sends no repeat pings.

2.7.21.5 Fail-Limit

This parameter defines the number of consecutive failed test series before the device is rebooted or the configured action is executed.

The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

0 … 4294967295

Default:

10

2.7.21.6 Boot-Type

The device executes this action if the ping to the target address was unsuccessful.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

Cold boot

The device performs a cold boot.

Warm boot

The device performs a warm boot.

Action

The device performs a configurable action. Configure the action under `/Setup/TCP-IP/Alive-Test` (also see *Action*).

Default:

Warm boot

2.7.21.7 Action

Here you enter the action executed by the device when the target address is unreachable. You can use the same actions as used in the cron table, i.e. executing CLI commands, HTTP requests, or sending messages.

The action set here will only be executed if the boot type is set to the value **Action**. The boot type is configured under **Setup** > **TCP-IP** > **Alive-Test** > **Boot-Type** (also see *Boot-Type*).

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

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

Default:

empty

2.7.21.8 Loopback-Address

Assign a loopback address (name of an ARF network, named loopback address or IP address) to be used for the alive test.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

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

Default:

empty

2.7.21.9 Reestablish-Action

Any command that can be executed on the command line can be specified as a restore action. If the device is in an error state where it cannot reach the target address, this command is executed once when the target address can be reached again.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

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

Default:

empty

2.7.21.11 Target-Address-2

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

Max. 15 characters from `[0-9].`

2.7.21.12 Target-Address-3

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

Max. 15 characters from `[0-9].`

2.7.21.13 Target-Address-4

One of four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the alive test to be considered successful.

Console path:

Setup > **TCP-IP** > **Alive-Test**

Possible values:

Max. 15 characters from `[0-9].`

2.7.22 ICMP-on-ARP-Timeout

When the device receives a packet that it should transmit to the LAN, it uses ARP requests to determine the recipient. If a request goes unanswered, the device returns a "ICMP host unreachable" message to the sender of the packet.

Console path:

Setup > **TCP-IP**

2.7.30 Network list

This table is used to define IP networks. These are referenced from other modules (DHCP server, RIP, etc.) via the network names.

Console path:

Setup > **TCP-IP**

2.7.30.1 Network-Name

Enter a unique name with max. 16 characters that the other modules (DHCP server, RIP, etc.) can use to reference the network.

The network name must not be the same as the name of a remote site (e.g. a VPN connection). Otherwise the communication on the network and the remote site won't be reliable anymore.

The network name must contain at least one letter as otherwise in the routing table there is no way to distinguish between IP address and interface.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

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

Default:

empty

2.7.30.2 IP address

If you use a private address range in your local network, then enter a valid and available IP address from this range here. IP masquerading conceals these addresses from remote networks, and these see only the Internet IP address of the corresponding remote station.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.7.30.3 IP-Netmask

If the intranet IP address you entered is an address from a private address range, then enter the associated netmask here.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

255.255.255.0

2.7.30.4 VLAN-ID

A single physical interface can be used to connect multiple separate VLANs (which were separated by a switch previously). The router must be given its own address and/or its own network in each of these VLANs. For this purpose, the interfaces and also a VLAN can be assigned to each network. If a packet is received on an interface with this VLAN ID, then the packet is assigned to the respective network, i.e. the network is only accessible for packets that come from the same VLAN. Packets coming from this network will be marked with this VLAN ID when being sent. A "0" stands for an untagged network (no VLAN).

Please note: Changing the ID is very dangerous. It is very easy to lock yourself out of the device if you do not have access to the VLAN. Also note that this setting affects all of the traffic managed by this network. This includes all packets that are routed through this network.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

0 … 4094

Default:

0

2.7.30.6 Src-check

This setting influences the address check by the firewall. "Loose" does not expect a return route, so any source address is accepted when the device is contacted. Thus the device can be accessed directly, as before. 'Strict', on the other hand, expects an explicit route if no IDS alerts are to be triggered.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

Loose
Strict

Default:

Loose

2.7.30.7 Type

Use this item to choose the type of the network (Intranet or DMZ) or disable it.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

Deactivated
Intranet
DMZ

Default:

Intranet

2.7.30.8 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received on this network are marked internally with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules. This tag also has an influence on the routes propagated by IP.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

0 … 65535

Default:

0

2.7.30.9 Comment

You can enter a comment here.

Console path:

Setup > **TCP-IP** > **Network-List**

Possible values:

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

Default:

empty

2.7.33 ARP-Bridge-Optimization

Switch for optimizing bridge negotiations for IPv4 and ARP.

Console path:

Setup > **TCP-IP**

Possible values:

No

For a packet received on a bridge link, the ARP stores the bridge information only. The switch port is set to 0. This forces the bridge to perform a MAC address lookup to find the actual link (and switch port).

Yes

The ARP stores the LAN information and switch port of the received ARP request/replies in the ARP table, regardless of whether the packet was received on a bridge link.

Default:

Yes

2.8 IP router

This menu contains the settings for the IP router.

Console path:

Setup

2.8.1 Operating

Switches the IP router on or off.

Console path:

Setup > **IP-Router**

Possible values:

Yes

The IP router is switched on.

No

The IP router is switched off.

Default:

No

2.8.2 IP-Routing-Table

In this table you enter the remote sites which are to be used for accessing certain networks or stations.

Console path:

Setup > **IP-Router**

2.8.2.1 IP address

This is where you specify the valid IP address as the destination address for this route. This can be an individual station that you wish to integrate into your network, or an entire network that you wish to couple with your own network.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

2.8.2.2 IP-Netmask

Specify here the netmask associated with the IP addresses entered. If you only need to translate one single IP address, enter the netmask `255.255.255.255`.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

2.8.2.3 Peer-or-IP

Select the router that the packets for this route should be forwarded to.

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

If this route is to lead to another station in the local network, simply enter the station's IP address.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

2.8.2.4 Distance

Enter the number of hops to this router You do not normally need to set this value as it is managed by the router automatically.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

0 … 16

Default:

0

2.8.2.5 Masquerade

You can use IP masquerading to hide a hide a logical network behind a single address (that of the router). If, for example, you have an Internet connection, you can us it to connect your entire network to the Internet.

Most Internet providers assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned fixed IP addresses, you can assign them to the relevant connection in the IP parameter list.

Select "on" to enable IP masquerading for all LAN interfaces. If you wish to assign fixed IP addresses to computers in the demilitarized zone (DMZ) and yet you still wish to activate IP masquerading for the computers on the other LAN interfaces (intranet), then select "Intranet".

If you want this entry to mask a VPN connection, select "on".

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

No

IP masking off

On

Intranet and DMZ masquerading

Intranet

Intranet - Intranet masquerading only

Default:

No

2.8.2.6 Operating

Specify the switch status here. The route can be activated and either always propagated via RIP or only propagated via RIP when the destination network can be reached.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

Yes: The route is activated and will always be propagated by RIP (sticky).
Semi: The route can be activated and is propagated via RIP when the destination network can be reached (conditional).
No: The route is off.

Default:

Yes: The route is activated and will always be propagated by RIP (sticky).

2.8.2.7 Comment

This field is available for comments.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

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

Default:

empty

2.8.2.8 Rtg-Tag

If you specify a routing tag for this route, then the route will be used exclusively for packets given the same tag by the firewall or arriving from a network with the corresponding interface tag.

It follows that the use of routing tags only makes sense in combination with corresponding, decorative rules in the firewall or tagged networks.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

0 … 65535

Default:

0

2.8.2.9 Admin-Distance

Administrative distance for this route. The default is 0 (set automatically by the operating system). The administrative distance parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route.

Console path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

0 … 255

Default:

0

2.8.5 Proxy-ARP

This is where you can activate/deactivate the ARP mechanism . Use proxy ARP to integrate remote computers into your local network as if they were connected locally.

Console path:

Setup > **IP-Router**

Possible values:

Yes

The proxy ARP mechanism is enabled.

No

The proxy ARP mechanism is disabled.

Default:

No

2.8.6 Send ICMP redirect

This is where you can chose if ICMP redirects should be sent.

Console path:

Setup > **IP-Router**

Possible values:

Yes

ICMP redirects are sent.

No

ICMP redirects are not sent.

Default:

Yes

2.8.7 Routing method

This menu contains the configuration of the routing methods used by your IP router.

Console path:

Setup > **IP-Router**

2.8.7.1 Routing method

Controls the analysis of ToS or DiffServ fields.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Normal

The TOS/DiffServ field is ignored.

Type of service

The TOS/DiffServ field is regarded as a TOS field; the bits "low delay" and "high reliability" will be evaluated.

DiffServ

The TOS/DiffServ field is regarded as a DiffServ field and evaluated as follows.

- **CSx (including CS0 = BE):** Normal transmission
- **AFxx:** Secure transmission
- **EF:** Preferred transmission

Default:

DiffServ

2.8.7.2 ICMP-Routing-Method

Specify if the router should transmit secure ICMP packets.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Normal

ICMP packets are transmitted unsecured.

Secured

ICMP packets are transmitted secured.

Default:

Normal

2.8.7.3 SYN/ACK-Speedup

Specify if TCP SYN and ACK packets should be given preferential treatment when forwarding.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Yes

TCP-SYN and ACK packets are forwarded preferentially.

No

TCP-SYN and ACK packets are not forwarded preferentially.

Default:

Yes

2.8.7.4 L2-L3-Tagging

Specify what should happen with DiffServ layer 2 tags.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Ignore
Yes - Copy to layer 3
Auto - Copy automatically

Default:

Ignore

2.8.7.5 L3-L2-Tagging

Here you specify whether DiffServ layer 3 tags should be copied to layer 2.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Yes
No

Default:

No

2.8.7.6 Route-Internal-Services

This is where you select whether the internal services are to be directed via the router.

You should treat the internal services VPN and PPTP specially since routing all packets without exception will result in performance loss. The device only forwards the initial packets sent by these services to the router while the connection is being established if you activate this option. Further packets are forwarded to the next port.

Console path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Yes

Packets for internal services are directed via the router.

No

Packets are returned straight to the sender.

Default:

No

2.8.8 RIP

This menu contains the RIP configuration for your IP router.

Console path:

Setup > **IP-Router**

2.8.8.2 R1-Mask

This setting is only required if you selected RIP-1 as RIP support. It affects how network masks are formed for routes learned on the basis of RIP.

Console path:

Setup > **IP-Router** > **RIP**

Possible values:

Class
Address
Class + address

Default:

Class

2.8.8.4 WAN sites

Here you configure the WAN-side RIP support separately for each remote site.

Console path:

Setup > **IP-Router** > **RIP**

2.8.8.4.1 Peer

From the list of specified peers, select the peer that sends the WAN-RIP packets that are to be learned.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

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

Special values:

*****

Multiple remote sites can be configured in one entry by using "*" as a place holder. If for example multiple remote stations are to propagate their networks via WAN RIP, while the networks for all other users and branch offices are defined statically, the appropriate remote stations can be given names with the prefix "RIP_". To configure all of the remote stations, the WAN RIP table requires just a single entry for remote station "RIP_*".

Default:

empty

2.8.8.4.2 RIP type

The RIP type details the RIP version with which the local routes are propagated.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

Off
RIP-1
RIP-1 compatible
RIP-2

Default:

Off

2.8.8.4.3 RIP accept

The column RIP accept lists whether RIP from the WAN is to be accepted. The RIP type must be set for this.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

Yes

RIP is accepted from the WAN.

No

RIP is not accepted from the WAN.

Default:

No

2.8.8.4.4 Masquerade

The column Masquerade lists whether or not masquerading is performed on the connection and how it is carried out. This entry makes it possible to start WAN RIP even in an empty routing table.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

Auto

The masquerade type is taken from the routing table. If there is no routing entry for the remote site, then masquerading is not performed.

On

All connections are masqueraded.

Intranet

IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently.

Default:

On

2.8.8.4.5 Dft-Rtg-Tag

The column Default tag lists the valid "Default routing tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

0 … 65535

Default:

0

2.8.8.4.6 Rtg-Tag-List

The column Routing tags list details a comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then only the tags in this list are accepted. When sending tagged routes on the WAN, only routes with valid tags are propagated.

All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

Max. 33 characters from `[0-9],`

Default:

empty

2.8.8.4.7 Poisoned reverse

Poisoned reverse prevents the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

On
Off

Default:

Off

2.8.8.4.8 RFC2091

Other than in the LAN, WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN once only when the connection is established. After this, updates only are transmitted (triggered updates).

Because updates are explicitly requested here, broadcasts or multicasts are not to be used for delivering RIP messages. Instead, the the subsidiary device must be statically configured with the IP address of the next available router at the

central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it then sends any messages on route changes directly to the subsidiary device.

In a central gateway, the setting "RFC 2091" can always be off and the "Gateway" entry always set to `0.0.0.0` because the central gateway always considers the gateway as specified at the subsidiary.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

On
Off

Default:

Off

2.8.8.4.9 Gateway

Valid IP address of the nearest available router in the context of RFC 2091.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

Special values:

0.0.0.0

If 0.0.0.0 is entered, the gateway address is determined from PPP negotiation.

In a router at the central location, RFC 2091 can be switched off and the gateway can remain on `0.0.0.0` because the central location always observes the requests from the subsidiaries.

The device automatically reverts to standard RIP if the gateway indicated does not support RFC 2091.

In a central gateway, the setting "RFC 2091" can always be off and the "Gateway" entry always set to `0.0.0.0` because the central gateway always considers the gateway as specified at the subsidiary.

2.8.8.4.10 RX filter

From the list of specified TIP filters, select the filter that is to be used when receiving RIP packets.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

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

Default:

empty

2.8.8.4.11 TX filter

From the list of specified TIP filters, select the filter that is to be used when sending RIP packets.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

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

Default:

empty

2.8.8.4.12 RIP-Send

Specify whether RIP is to be propagated on the WAN routes. The RIP type must be set for this.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

No
Yes

Default:

No

2.8.8.4.13 Loopback address

Enter a loopback address here. Possible values are:

- The name of an ARF network
- Configured loopback address
- IPv4 address

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Table**

Possible values:

Specify a valid IPv4 address here.

Default:

empty

2.8.8.4.14 Ignore-Tags

This entry controls the learning and propagation behavior operated on this interface.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

No

Yes

With this setting, routes are learned with the "Dft-Rtg-Tag" configured for the interface and propagated with the tag 0 assuming that they contain tags allowed by the tag list for this interface and have networks that are allowed by the respective filters.

Default:

No

2.8.8.5 LAN sites

This table is used to adjust RIP settings and to select the network that they apply to.

Console path:

Setup > **IP-Router** > **RIP**

2.8.8.5.1 Network name

Select here the name of the network to which the settings are to apply.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Intranet
DMZ
empty

Default:

2.8.8.5.2 RIP type

Specify whether the router should support IP-RIP or not. IP-RIP can be used to exchange routing information between individual stations automatically.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Off
RIP-1
RIP-1 compatible
RIP-2

Default:

Off

2.8.8.5.3 RIP accept

Specify here whether routes from this network should be learned or not.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Yes
No

Default:

No

2.8.8.5.4 Propagate

This option defines whether the associated network is to be propagated to other networks.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Yes
No

Default:

No

2.8.8.5.5 Dft-Rtg-Tag

Enter a value here for the default routing tag that is valid for the selected interface. Routes that have the interface tag set will be propagated on this interface with the default routing tag. Routes learned by the interface that have this default routing tag set will be added to the RIP table with the interface tag. In addition, unmarked routes (i.e. routes with tag `0`) will not be propagated on this interface unless the interface itself has the tag `0`.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

0 … 65535

Default:

0

2.8.8.5.6 Rtg-Tag-List

This field contains a comma-separated list of routing tags that are accepted by this interface. If this list is empty, then all routes are accepted irrespective of their routing tags. If the list contains at least one tag, then only the tags in this list are accepted. Similarly, when marked routes are being sent, only routes with permitted tags (i.e. those listed here) are forwarded. The routing tag list corresponds insofar to the WAN RIP list with the difference that any realization using standard routing is also taken into account. This means for example that, in the case of an interface tag '1' and the standard routing tag '0', the tag '0' has to be included in the routing tag list because it is internally changed to tag '1' when it is received. When transmitted, the internal tag '1' is converted into the external tag '0'. This measure is necessary in order for a virtualized router to be able to work together with other routers in the LAN that do not support tagged routes.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Max. 33 characters from `[0-9],`

Default:

empty

2.8.8.5.7 Poisoned reverse

Poisoned reverse prevents the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

Yes
No

Default:

No

2.8.8.5.10 RX filter

Specify here the filter to be applied when receiving (RX) RIP packets.

You must first define the filter in the RIP filter list in order to use it here.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

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

Default:

empty

2.8.8.5.11 TX filter

Specify here the filter to be applied when sending (TX) RIP packets.

You must first define the filter in the RIP filter list in order to use it here.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

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

Default:

empty

2.8.8.5.12 RIP-Send

Specify here whether routes should be propagated in this network. The RIP type must be set for this.

Console path:

Setup > **IP-Router** > **RIP** > **LAN-Sites**

Possible values:

No
Yes

Default:

No

2.8.8.5.14 Ignore-Tags

This entry controls the learning and propagation behavior operated on this interface.

Console path:

Setup > **IP-Router** > **RIP** > **WAN-Sites**

Possible values:

No
Yes

With this setting, routes are learned with the "Dft-Rtg-Tag" configured for the interface and propagated with the tag 0 assuming that they contain tags allowed by the tag list for this interface and have networks that are allowed by the respective filters.

Default:

No

2.8.8.6 settings

The Routing Information Protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information.

Console path:

Setup > **IP-Router** > **RIP**

2.8.8.6.1 Update

The time between two regular updates. A random value of +/-5 seconds is always added to this value.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

10 … 99 Seconds

Default:

30

2.8.8.6.2 Holddown

The holddown interval defines how many update intervals pass before a route from router A which is no longer being propagated is replaced by an inferior route from router B.

The device will only accept a route from the same router that propagated the original route until the holddown interval expires. Within this period, the device only accepts a route from another router if it is better than the former route.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

0 … 99 as multiples of the update interval

Default:

4

2.8.8.6.3 Invalidate

The invalidate interval defines the number of update intervals before a route is marked as invalid (unavailable) when it stops being propagated by the router that originally reported it.

If the device learns of an equivalent or better route from another router within this time period, then this will be used instead.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

0 … 99 as multiples of the update interval

Default:

6

2.8.8.6.4 Flush

If a route in a router is not updated before the flush interval expires, then the route is deleted from the dynamic routing table.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

0 … 99 as multiples of the update interval

Default:

10

2.8.8.6.5 Upd-Delay

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay stops faulty configurations from causing excessive update messages.

The update delay starts as soon as the routing table, or parts of it, are propagated. As long as this delay is running, new routing information is accepted and entered into the table but it is not reported any further. The router actively reports its current entries only after expiry of this delay.

The value set here sets the upper limit for the delay – the actual delay is a random value between one second and the value set here.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

1 … 99 Seconds

Default:

5

2.8.8.6.6 Max-Hopcount

In some scenarios it may be desirable to use a larger maximum hop count than that intended by RIP (16). This value can be adapted with the parameter Max Hopcount.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

16 … 99

Default:

16

2.8.8.6.7 Routes-per-Frame

The number of routes that can be propagated in a single packet.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

1 … 99

Default:

25

2.8.8.6.8 Inter-Packet-Delay

If the number of devices on the network is so high that they no longer fit into a single RIP packet, the sending router divides this into multiple RIP packets. In order for low-end routers on the network to be able to handle the successive RIP packets, you configure a delay in milliseconds between the individual RIP packets here.

Console path:

Setup > **IP-Router** > **RIP** > **Parameter**

Possible values:

Max. 3 characters from `0123456789`

0 … 255 Milliseconds

Default:

0

2.8.8.7 Filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses (e.g. "Only learn routes in the network 192.168.0.0/255.255.0.0"). First of all a central table is used to define the filters that can then be used by entries in the LAN and WAN RIP table.

Filters defined in the filter table can be referenced in the columns for RX filter and TX filter in the LAN RIP and WAN RIP tables. RX defines the networks from which routes can be learned or blocked, and TX defines the networks to which propagation should be allowed or blocked.

Console path:

Setup > **IP-Router** > **RIP**

2.8.8.7.1 Name

Name of the filter.

The hash symbol # can be used to combine multiple entries into a single filter. Taken together, the entries LAN#1 and LAN#2 make up a filter "LAN" that can be called from the RIP table.

Console path:

Setup > **IP-Router** > **RIP** > **Filter**

Possible values:

Max. 18 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.8.8.7.2 Filter

Comma-separated list of networks that are to be accepted (+) or rejected (-).

The plus-sign for accepted networks is optional.

Filtering by routing tags is unaffected, i.e. if a tag for a route indicates that it is not to be learned or propagated, then this cannot be forced by means of the filter table.

Console path:

Setup > **IP-Router** > **RIP** > **Filter**

Possible values:

Max. 64 characters from `[0-9]+-,`

Default:

empty

2.8.8.8 Best routes

In large networks a destination network may be reachable via several gateways. If all these gateways propagate their routes using RIP the device will learn several routes to the same destination. The preferred routes are stored in the "Best Routes" table. This table contains the following entries:

- IP address
- IP-Netmask
- Rtg-Tag
- Gateway
- Distance
- Time
- Peer
- Port
- VLAN-ID
- Network name

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.1 IP address

The IP address of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.2 IP-Netmask

The IP address of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.3 Time

The time required to reach the network via this route.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.4 Distance

Th distance to the network to which the route belongs (i.e. the number of intermediate hops).

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.5 Gateway

The gateway via which the network can be reached to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.6 Rtg-Tag

The routing tag of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.8 Peer

Remote device that can be reached over this route.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.10 VLAN-ID

The VLAN ID of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.11 Network name

The name of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.8.12 Port

The (logical) LAN interface via which the route was learned.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9 All routes

In large networks a destination network may be reachable via several gateways. If all these gateways propagate their routes using RIP the device will learn several routes to the same destination. These routes are stored in the "All Routes" table. This table contains the following entries:

- IP address
- IP-Netmask
- Rtg-Tag
- Gateway
- Distance
- Time
- Peer
- Port
- VLAN-ID
- Network name

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.1 IP address

The IP address of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.2 IP-Netmask

The IP address of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.3 Time

The time required to reach the network via this route.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.4 Distance

Th distance to the network to which the route belongs (i.e. the number of intermediate hops).

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.5 Gateway

The gateway via which the network can be reached to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.6 Rtg-Tag

The routing tag of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.8 Peer

Remote device that can be reached over this route.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.10 VLAN-ID

The VLAN ID of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.11 Network name

The name of the network to which the route belongs.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.8.9.12 Port

The (logical) LAN interface via which the route was learned.

Console path:

Setup > **IP-Router** > **RIP** > **Best-Routes**

2.8.9 1-N-NAT

This menu contains the configuration of 1-N-NAT for your IP router.

Console path:

Setup > **IP-Router**

2.8.9.1 TCP-Aging-Seconds

The connection list keeps track of open TCP sessions for any communication passing through the router, so that these can be mapped correctly during communication. Usually a TCP connection is closed after the communication is completed. In some cases it can occur that a TCP connection isn't closed by the initiator or the responder. As the connection list would get overloaded and performance would thus decrease, TCP connections are closed after the timer “TCP aging” has expired.

Enter a value here in seconds after which the corresponding entry of a TCP connection in the connection list will be deleted when idle.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

0 … 65535 Seconds

Default:

300

2.8.9.2 UDP-Aging-Seconds

Specify here how long an IPsec connection is inactive before the corresponding entry in the masquerading table is deleted.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

0 … 65535 Seconds

Default:

120

2.8.9.3 ICMP-Aging-Seconds

Specify here how long an IPSec connection is inactive before the corresponding entry in the masquerading table is deleted.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

0 … 65535 Seconds

Default:

10

2.8.9.4 Service table

If you wish to make certain services or stations accessible from outside of your network (e.g. a web server), enter these services and stations in this table.

Console path:

Setup > **IP-Router** > **1-N-NAT**

2.8.9.4.1 D-port-from

Specify the port of the desired service here.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

1 … 65535

2.8.9.4.2 Intranet-Address

Enter the valid IP address of the computer in the intranet providing the service.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

0 … 65535

Default:

0

2.8.9.4.3 D-port-to

Specify the port of the desired service here.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

1 … 65535

2.8.9.4.4 Map-Port

Port used for forwarding the packet.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

0 … 65535

Default:

0

2.8.9.4.5 Active

You can set this entry temporarily inactive without having to delete it.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

Yes

Enables this entry.

No

Disables this entry.

Default:

Yes

2.8.9.4.6 Comment

This field is available for comments.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

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

Default:

empty

2.8.9.4.7 Peer

From the list of specified peers, select the peer that applies to this entry.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

2.8.9.4.8 Protocol

Here you define which protocol the dataset applies to.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

Possible values:

TCP
UDP
TCP+UDP

Default:

TCP+UDP

2.8.9.4.9 WAN address

Here you define which WAN address the dataset applies to. Where more than one static IP address is available, specifying this address enables a targeted port forwarding to be achieved for this address. If the address `0.0.0.0` is specified, then the address assigned to the connection will continue to be used.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Service-Table**

2.8.9.5 Table-1-N-NAT

The 1-N-NAT table shows the masked connections.

Console path:

Setup > **IP-Router** > **1-N-NAT**

2.8.9.5.1 Intranet-Address

Shows the valid internal IP address of the station to which a masked connection has been stored.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.2 Source-Port

Source port of the masked connection.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.3 Protocol

Protocol (UDP/TCP) used by the masked connection.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.4 Timeout

Lease period for the masked connection in seconds (set under TCP aging, UDP aging or ICMP aging).

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.5 Handler

Handler required for masking, e.g. FTP

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.6 Remote address

Valid remote IP address that the masked connection was connected to.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.5.7 WAN address

WAN address used for this connection.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **Table-1-N-NAT**

2.8.9.6 Fragments

This setting controls the firewall's behavior regarding fragmented IP packets.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

Filter

Fragments are always dropped (filtered).

Route

The fragments are demasked. However, the fragments must be received in their original order. In addition, this settings allows only the individual fragments to be checked by the firewall, and not the entire IP packet.

Reassemble

The fragments are stored temporarily until the IP packet can be reassembled in full. The fragments may be received in any order. The firewall also checks the reassembled IP packet.

Default:

Reassemble

2.8.9.7 Fragment-Aging-Seconds

If an IP packet cannot be fully desmasked because fragments are missing, this time in seconds determines when the incomplete fragments are dropped.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

1 … 255

Default:

5

2.8.9.8 IPSec-Aging-Seconds

Specify here how long an IPSec connection is inactive before the corresponding entry in the masquerading table is deleted.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

0 … 65535 Seconds

Default:

2000

2.8.9.9 IPSec-Table

The IPSec table displays the masked IPSec connections, including some of the connection parameters.

Console path:

Setup > **IP-Router** > **1-N-NAT**

2.8.9.9.1 Remote address

Valid IP address of the remote VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.2 Local address

Valid IP address of the local VPN gateway (generally a VPN client in the local network)

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.3 rc-hi

The most significant 32 bits of the IKE cookie of the remote VPN gateway.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.4 rc-lo

The least significant 32 bits of the IKE cookie of the remote VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.5 lc-hi

The most significant 32 bits of the IKE cookie of the local VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.6 lc-lo

The least significant 32 bits of the IKE cookie of the local VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.7 Remote SPI

SPI used by the remote VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.8 Local SPI

SPI used by the local VPN gateway

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.9 Timeout

Timeout in seconds until the entry is deleted. The value is set under **IPSec-Aging-Seconds**. The default value is 2000 seconds.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.10 Flags

Flags that describe the state of the connection:

0x01

Connection is inverse masqueraded.

0x02

Connection waits for SPI.

0x04

Other connections wait for SPI.

0x08

Aggressive mode connection.

0x10

NAT-traversal connection.

0x20

Session recovery

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.11 CO

Connect timeout. Runs straight after the entry is created. If no SA is negotiated within 30 seconds (i.e. no ESP packet is sent or received) the entry is deleted again.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.12 NL

Local notification timeout. This timer is started when an IKE notification is received from the local VPN gateway. The entry is deleted if no IKE or ESP packet is received from the remote site within 30 seconds.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.13 NR

Remote notification timeout: Corresponds to the local notification timeout, except that in this case the notification was received from the remote VPN gateway.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.14 DP

DPD timeout: This timer is started when a DPD packet is received from one site. If no DPD packet is received from the other site within 30 seconds the entry is removed.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.9.15 WAN address

WAN address used for this connection.

Console path:

Setup > **IP-Router** > **1-N-NAT** > **IPSec-Table**

2.8.9.10 ID-Spoofing

NAT replaces the packet IDs in the outbound packets (ID spoofing). This enables fragmented packets to be transmitted and it stops information on the internal network (packet IDs) from being leaked to the outside. If AH is being used, this procedure should be avoided as the packet IDs are required by AH. For AH to function properly, ID spoofing can be deactivated here.

Console path:

Setup > **IP-Router** > **1-N-NAT**

Possible values:

Yes
No

Default:

Yes

2.8.10 Firewall

This menu contains the firewall configuration.

Console path:

Setup > **IP-Router**

2.8.10.1 Objects

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

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

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.1.1 Name

Specify here a unique name for this object.

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

Console path:

Setup > **IP-Router** > **Firewall** > **Objects**

Possible values:

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

Default:

empty

2.8.10.1.2 Description

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

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

Table 11: Objects for firewall actions

Description	Object-ID	Examples and comments
Local network	`%L`	
Remote sites	`%H`	Name must be in DSL/ISDN/PPTP or VPN remote site list
Host name	`%D`	
MAC-Address	`%E`	`00:A0:57:01:02:03`
IP-Address	`%A`	`%A10.0.0.1, 10.0.0.2`; `%A0` (all addresses)
Netmask	`%M`	`%M255.255.255.0`
Protocol (TCP/UDP/ICMP, etc.)	`%P`	`%P6` (for TCP)
Service (port)	`%S`	`%S20-25` (for ports 20 to 25)
LANCOM Trusted Access	`%g`	The UUID for objects of the LANCOM Trusted Access must meet the following criteria: › They may only contain hexadecimal numbers ('0'…'9', 'a'…'f', 'A'…'F') and the minus sign ('-'). › The minus may only be at propositions 8, 13, 18 and 23 › The minus character must appear 4 times in total › The UUID must be at least 36 characters long

Description	Object-ID	Examples and comments
		Example: 550e8400-e29b-11d4-a716-446655440000

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

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

Console path:

Setup > **IP-Router** > **Firewall** > **Objects**

Possible values:

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

Default:

empty

2.8.10.2 Rules

The rules table links various pieces of information on a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules, and activation of the rule for VPN connections.

LCOS has a special syntax to define firewall rules. This syntax enables the representation of complex interrelationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the LCOS syntax every time:

The firewall actions are stored in the action table

The object table holds the stations and services

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate LCOS syntax (e.g. %P6 for TCP).

The objects from these tables can be used for rule definition, although this is not compulsory. They merely simplify the use of frequently used objects. For direct input of level parameters in the LCOS syntax, the same rules apply as specified in the following sections for protocols, source/destination and firewall actions.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.2.1 Name

Specify here a unique name for this firewall rule.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

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

Default:

empty

2.8.10.2.2 Prot.

Specification of the protocols for which this entry is to apply.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

Direct entry in LCOS syntax as described in the *Objects* table.
Link to an entry of the object table.

2.8.10.2.3 Source

Specification of the source stations for which this entry is to apply.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

Direct entry in LCOS syntax as described in the *Objects* table.
Link to an entry of the object table.

2.8.10.2.4 Destination

Specification of the destination stations for which this entry is to apply.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

Direct entry in LCOS syntax as described in the *Objects* table.
Link to an entry of the object table.

2.8.10.2.7 Action

Action to be run if the firewall rule applies to a packet.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

Direct entry in LCOS syntax as described in the *Actions* table.
Link to an entry of the action table.

2.8.10.2.8 Linked

Links the rule to other rules.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

No
Yes

Default:

No

2.8.10.2.9 Prio

Priority of the rule.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

0 … 255

Default:

empty

2.8.10.2.10 Operating

Switches the rule on/off.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

No
Yes

Default:

Yes

2.8.10.2.11 VPN rule

Activates the rule for creating VPN rules.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

No
Yes

Default:

No

2.8.10.2.12 Stateful

When this option is enabled, a check is performed as to whether a connection is being established correctly. Erroneous packets are dropped whilst the connection is being established. If this option is disabled, all packets for which this rule applies are accepted.

Furthermore, this option is enabled for the automatic protocol recognition for FTP, IRC, PPTP necessary to be able to open a port in the firewall for each data connection.

The test for portscans/SYN flooding is also enabled/disabled with this option. This can exclude particular, heavily-frequented servers from the test, meaning that limits for half-open connections (DOS) or port requests (IDS) do not have to be set so high that they effectively become useless.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

No
Yes

Default:

Yes

2.8.10.2.13 Comment

This field is available for comments.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

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

Default:

empty

2.8.10.2.14 Rtg-Tag

Routing tag for the rule.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

0 … 65535

Default:

0

2.8.10.2.15 Src-Tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received. This can be used to restrict firewall rules to certain ARF contexts.

1 to 65534

The firewall rule is applied if the expected interface- or routing tag is 1...65534.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

0 … 65535

Default:

0

Special values:

0

Wildcard. The firewall rule is applied to all ARF contexts (the expected interface- or routing tag is 0...65535).

65535

The firewall rule is applied if the expected interface- or routing tag is 0.

2.8.10.2.16 LB-Policy

Defines the Dynamic Path Selection Policy used for this firewall rule. This can either be one of the predefined ones from *2.8.20.4 Predefined-Selectors* on page 259 or one of the self-generated ones under *2.110.4.16 Policies* on page 1883.

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

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

Default:

empty

2.8.10.2.17 LB-Switchover

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

Console path:

Setup > **IP-Router** > **Firewall** > **Rules**

Possible values:

No
Yes

Default:

No

2.8.10.3 Filter list

The filter list is generated from the rules in the firewall. The filters it contains are static and can only be changed when firewall rules are added, edited or deleted..

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.3.1 Idx.

Index for this entry in the list.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.2 Prot.

TCP protocol for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.3 Source address

Valid source IP address for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.4 Source netmask

Source IP netmask for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.5 S-St.

Start address of range of source IP addresses whose data packets are processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.6 S-End

End address of the range of source IP addresses whose data packets are processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.7 Destination address

Valid destination IP address for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.8 Dst-netmask

Valid destination IP netmask for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.9 D-St.

Start address of range of destination IP addresses whose data packets are processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.10 D-End

End address of range of destination IP addresses whose data packets are processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.11 Action

Action performed for the data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.13 Source MAC

Source MAC address for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.14 Dst-MAC

Destination MAC address for data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.15 Linked

Indicates whether further firewall rules are applied after this action.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.16 Prio

Priority for this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.17 Rtg-Tag

This routing tag is added to data packets processed by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.3.18 Src-Tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received.

Console path:

Setup > **IP-Router** > **Firewall** > **Filter-List**

2.8.10.4 Action table

A firewall action comprises of a condition, a limit, a packet action and other measures.

As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.4.1 Name

Specify a unique name for this action.

Console path:

Setup > **IP-Router** > **Firewall** > **Actions**

Possible values:

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

Default:

empty

2.8.10.4.2 Description

In the actions table, firewall actions are combined as any combination of conditions, limits, packet actions and other measures.

A firewall action comprises of a condition, a limit, a packet action and other measures. In the actions table, firewall actions are made up of combinations of any of the following elements:

Console path:

Setup > **IP-Router** > **Firewall** > **Actions**

Possible values:

Conditions

Table 12: Conditions for firewall actions

Condition	Description	Object-ID
Connect filter	The filter is active if there is no physical connection to the destination of the packet	`@c`
DiffServ filter	The filter is active if the packet contains the specified Differentiated Services Code Point (DSCP)	`@d`
Internet-Filter	The filter is active if the packet was received, or is to be sent, via the default route	`@i`
VPN-Filter	The filter is active if the packet was received, or is to be sent, via a VPN connection	`@v`

If no further action is specified for the "Connect" or "Internet" filter, a combination of these filters is implicitly adopted with the "Reject" action.

Limits

Each firewall action can be associated with a limit, which triggers the action if it is exceeded. Action chains can be formed by combining multiple limits for a filter Limit objects are generally initiated with `%L` followed by:

Table 13: Limit objects for firewall actions

Relation	Connection-related (c) or global (g)
Type	Data rate (d), number of packets (p), or packet rate (b)
Limit value	The filter is active if the packet was received, or is to be sent, via the default route
Other parameters	e.g. time and size

2.8.10.5 Connection list

Established connections are entered into the connection list if the checked packet is accepted by the filter list. The connection list records the source and destination, the protocol, and the port that a connection is currently allowed to use. The list also indicates how long the entry remains in the list and which firewall rule generated the entry. This list is highly dynamic and always "on the move".

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.5.1 Source address

A valid IP address of the station that established a connection.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.2 Destination address

A valid destination IP address to which a connection was established.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.3 Prot.

Protocol allowed on this connection.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.4 Source port

Source port of the station that established a connection.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.5 Destination port

Destination port to which a connection was established.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.6 Timeout

Lease for this entry in the table.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.7 Flags

The flags are used to store information on the connection state and other (internal) information to a bit field.

The states can have the following values: New, establish, open, closing, closed, rejected (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST).

UDP connections know the states, open and closing (the latter only if the UDP connection is linked by a stateful control channel.

Console path:

Setup > **IP-Router** > **Firewall** > **Connection-List**

Possible values:

00000001 TCP
SYN sent.

00000002 TCP
SYN/ACK received.

00000004 TCP
Waiting for server ACK

00000008 all
Connection open.

00000010 TCP
FIN received.

00000020 TCP
FIN sent.

00000040 TCP
RST sent or received.

00000080 TCP
Session being restored.

00000100 FTP
Passive FTP connection being established.

00000400 H.323
Related T.120 connection.

00000800
Connection via loopback interface.

00001000
Check linked rules.

00002000
Rule is linked.

00010000
Destination is on "local route".

00020000
Destination is on default route.
00040000
Destination is on VPN route.
00080000
No physical connection established.
00100000
Source is on default route.
00200000
Source is on VPN route.
00800000
No route to destination.
01000000
Contains global action with condition.

2.8.10.5.8 Filter rule

Shows the filter rule that generated the entry.

Console path:
Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.9 Source route

Source route used to establish this connection.

Console path:
Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.10 Destination route

Destination route to which a connection was established.

Console path:
Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.5.11 Rtg-Tag

Connection routing tag.

Console path:
Setup > **IP-Router** > **Firewall** > **Connection-List**

2.8.10.6 Host blocking list

The port blocking list contains those stations that are blocked for a certain time due to a firewall event. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.6.1 Source address

Valid source IP address that is blocked by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Host-Block-List**

2.8.10.6.2 Timeout

Lease for this entry in the table.

Console path:

Setup > **IP-Router** > **Firewall** > **Host-Block-List**

2.8.10.6.3 Filter rule

Shows the filter rule that generated the entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Host-Block-List**

2.8.10.7 Port blocking list

The port blocking list contains those protocols and services that are blocked for a certain time due to a firewall event. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.7.1 Destination address

Valid destination IP address that is blocked by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Port-Block-List**

2.8.10.7.2 Prot.

Protocol that is blocked by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Port-Block-List**

2.8.10.7.3 Destination port

Destination port blocked by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Port-Block-List**

2.8.10.7.4 Timeout

Lease for this entry in the table.

Console path:

Setup > **IP-Router** > **Firewall** > **Port-Block-List**

2.8.10.7.5 Filter rule

Shows the filter rule that generated the entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Port-Block-List**

2.8.10.8 Max.-Half-Open-Conns.

Denial-of-Service attacks take advantage of inherent weaknesses in the TCP/IP protocol in combination with poor implementations. Attacks which target these inherent weaknesses include SYN Flood and Smurf. Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land). Your device detects most of these attacks and reacts with appropriate countermeasures.

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

100 … 9999

Default:

100

2.8.10.9 DoS action

This is where you can specify what action should be taken with packets that activate or exceed the trigger. You can transfer the packets, drop them uncommented or reject them using ICMP reject (i.e. the sender is informed).

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Transmit
Drop
Reject

Default:

Drop

2.8.10.10 Admin-Email

If you wish to be notified of predefined events (DoS, IDS or when limits are exceeded) you must specify a valid e-mail address here.

For e-mail messaging, you have to enter the necessary settings into the main group **Log & Trace** in the subsection "SMTP".

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

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

Default:

empty

2.8.10.11 Operating

You can switch the entire firewall on or off here. The firewall inspects and counts every single incoming and outgoing packet. Depending on the protocol in question, it temporarily opens the channels that are required by a local station for processing a request. Furthermore individual networks, peers, services or protocols can be preferred, limited or blocked.

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Yes
No

Default:

Yes

2.8.10.12 Port-Scan-Threshold

Intrusion-Detection-System (IDS). Your device detects most unauthorized intrusion attempts and can respond with countermeasures that can be configured here.

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

50 … 9999

Default:

50

2.8.10.13 IDS action

This is where you can specify what action should be taken with packets that activate or exceed the trigger. You can transfer the packets, drop them uncommented or reject them using ICMP reject (i.e. the sender is informed).

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Transmit
Drop
Reject

Default:

Drop

2.8.10.14 Ping block

A controversial method of increasing security is to conceal the router by not responding to ping and traceroute requests (ping blocking). This is controversial because the failure to answer can also betray the existence of a device. If there truly is no device present, the previous router will respond to the relevant packets with 'undeliverable' as it is unable to deliver them. However, if the previous router no longer responds with a corresponding rejection, the packet is 'deliverable' and, regardless of the recipient's subsequent behavior, is most certainly present. It is not possible to simulate the behavior

of the previous router without keeping your device offline or switching it off (and thus making it unreachable for the services you yourself request).

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Off
Always
WAN
Default route

Default:

Off

2.8.10.15 Stealth-Mode

A controversial method of increasing security is to conceal the router by not conforming to standards and rejecting TCP and UDP requests, but by ignoring them (stealth mode) . This is controversial because the failure to answer can also betray the existence of a device. If there truly is no device present, the previous router will respond to the relevant packets with 'undeliverable' as it is unable to deliver them. However, if the previous router no longer responds with a corresponding rejection, the packet is 'deliverable' and, regardless of the recipient's subsequent behavior, is most certainly present. It is not possible to simulate the behavior of the previous router without keeping your device offline or switching it off (and thus making it unreachable for the services you yourself request).

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Off
Always
WAN
Default route

Default:

Off

2.8.10.16 Auth-Port

Hiding TCP or UDP ports will cause problems on masked connections where so-called “authenticate” or “ident” queries, as used by some mail and news servers to request additional information from users, are no longer rejected correctly. These servers then time out, resulting in considerable delays in the delivery of mail or news. In order to overcome this problem when stealth mode is switched on, stealth mode is deactivated temporarily for the port in question. The firewall recognizes that the internal station's wish to establish contact with a mail (SMTP, POP3, IMAP2) or news server (NNTP) and opens the port for 20 seconds. You can use this option to suppress the temporary deactivation of stealth mode for the authentication port.

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

stealth
No

Default:

stealth

2.8.10.17 Deny-Session-Recover

The firewall opens appropriate channels for each session initiated and its associated connections (e.g. FTP with control and data connections) for a certain period. If there is no communication over the connection for a defined period of time (setting in the IP router masquerading), then the session is considered to be ended and the channels associated with the connections are closed. Selecting 'session recover' determines the behavior of the firewall when receiving packets which appear to belong to an earlier session. The packets are dropped or it is assumed that a session existed but that no communication took place for too long. In this case, an equivalent session can be reestablished. The latter behavior can in general be allowed or forbidden. Denial of a session can be restricted to the default route or to WAN sessions.

This setting has no effect if the default route points to the LAN.

Console path:

Setup > **IP-Router** > **Firewall**

Possible values:

Off - always permitted
Always - always forbidden
WAN - forbidden over WAN
Default-route - forbidden on default route

Default:

Default-route - forbidden on default route

2.8.10.19 Open-Port-List

The port blocking list contains protocols and services that a firewall event has permitted for a certain time. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.19.1 Source address

Valid source IP address that can be used by the open ports and protocols in this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.2 Destination address

Valid destination IP address to which a connection may be established using the open ports and protocols in this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.3 Prot.

Protocol opened by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.5 Destination port

Destination port opened by this entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.6 Timeout

Lease for this entry in the table.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.8 Filter rule

Shows the filter rule that generated the entry.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.19.9 Source route

Source route used to establish this connection.

Console path:

Setup > **IP-Router** > **Firewall** > **Open-Port-List**

2.8.10.20 Applications

This menu contains the configuration of individual firewall applications.

Console path:

Setup > **IP-Router** > **Firewall**

2.8.10.20.1 FTP

This menu contains the configuration of FTP for your firewall.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications**

2.8.10.20.1.1 FTP block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'FTP block' specifies whether and on what routes any type of FTP should be given special treatment.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **FTP**

Possible values:

Off
Always
WAN
Default route

Default:

Off

2.8.10.20.1.2 Active-FTP-Block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'Block active FTP' specifies whether and on what routes active FTP should be given special treatment.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **FTP**

Possible values:

No
Always
WAN
Default route

Default:

No

2.8.10.20.1.3 Min-Port

When an FTP session is identified on any port, the countermeasures configured here are taken. 'Minimum port number' specifies the smallest permitted port for active FTP.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **FTP**

Possible values:

1024 … 9999

Default:

1024

2.8.10.20.1.4 Check-Host-IP

When an FTP session is identified on any port, the countermeasures configured here are taken. "Check host IP" specifies whether and on what routes the address transmitted in the FTP command should be checked against the source address of the FTP client. If it does not match, the countermeasures configured below will be taken. This check will of course be skipped if a site-to-site transfer is to take place and is permitted es.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **FTP**

Possible values:

No
Always
WAN
Default route

Default:

Default route

2.8.10.20.1.5 FXP block

When an FTP session is identified on any port, the countermeasures configured here are taken. 'FXP block' specifies whether site-to-site transfers (FXP) should be given special treatment.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **FTP**

Possible values:

No
Always
WAN
Default route

Default:

Default route

2.8.10.20.2 IRC

This menu contains the configuration of IRC for your firewall.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications**

2.8.10.20.2.1 IRC block

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Block IRC' specifies whether and on what routes any type of IRC should be given special treatment.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **IRC**

Possible values:

No
Always
WAN
Default route

Default:

No

2.8.10.20.2.2 DDC block

When an IRC session is identified on any port, the countermeasures configured here are taken. "Block DDC" specifies whether and on what routes Direct-Data-Connect (private chats and file transfers) should be given special treatment.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **IRC**

Possible values:

No
Always
WAN
Default route

Default:

No

2.8.10.20.2.3 Min-Port

When an IRC session is identified on any port, the countermeasures configured here are taken. 'Minimum port number' specifies the smallest permitted port for DDC.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **IRC**

Possible values:

1024 … 9999

Default:

1024

2.8.10.20.2.4 Check-Host-IP

When an IRC session is identified on any port, the countermeasures configured here are taken. "Check-Host-IP" indicates whether and on what routes the address transmitted in the DDC command should be checked against the source address of the IRC client.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications** > **IRC**

Possible values:

No
Always
WAN
Default route

Default:

Default route

2.8.10.20.10 Appl.-Action

When an IRC session is identified on any port, the countermeasures configured here are taken.

Console path:

Setup > **IP-Router** > **Firewall** > **Applications**

Possible values:

Transmit
Drop
Reject

Default:

Reject

2.8.11 Start-WAN-Pool

Enter a range of IP addresses that should be assigned to users dialing into the device..

Each user is automatically assigned a free address from this range. As soon as a user disconnects from the device, the assigned address is freed up and is available for other users.

Console path:

Setup > **IP-Router**

2.8.12 Ende-WAN-Pool

Enter a range of IP addresses that should be assigned to users dialing into the device..

Each user is automatically assigned a free address from this range. As soon as a user disconnects from the device, the assigned address is freed up and is available for other users.

Console path:

Setup > **IP-Router**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.8.19 N-N-NAT

The rules in the N:N-NAT table regulate the IP addresses to which source addresses or entire IP networks are translated. These rules must be specified explicitly for each remote site because translation takes place after routing. The remote site reaches the stations or networks at their translated IP address as specified.

Console path:

Setup > **IP-Router**

2.8.19.1 Idx.

The rules in the N:N-NAT table regulate the IP addresses to which source addresses or entire IP networks are translated. These rules must be specified explicitly for each remote site because translation takes place after routing. The remote site reaches the stations or networks at their translated IP address as specified.

Console path:

Setup > **IP-Router** > **N-N-NAT**

Possible values:

Max. 4 characters from `[0–9]`

Default:

empty

2.8.19.2 Source address

Valid IP address of the computer or network that is to receive an alternative IP address.

Console path:

Setup > **IP-Router** > **N-N-NAT**

2.8.19.3 Source mask

Netmask of the source range.

Console path:

Setup > **IP-Router** > **N-N-NAT**

2.8.19.4 Destination station

From the list of specified remote stations, select the remote device that can be used to access the remote network.

Console path:

Setup > **IP-Router** > **N-N-NAT**

2.8.19.5 Mapped-Network

IP addresses or address range to be used for translation.

For the new network address, the same netmask is taken as used by the source address. The following applies with the assignment of source and mapping addresses:

- When translating individual addresses, source and mapping can be assigned in any way.
- When entire address ranges are translated, the computer-related part of the IP address is used directly and only the network-related part of the mapping address is appended. When assigning `10.0.0.0`/`255.255.255.0` to `192.168.1.0`, the server in the LAN with the IP address `10.1.1.99` is necessarily assigned with the mapping address `192.168.1.99`.

The address range for translation must be at least as large as the source address range.

Please note that the N:N mapping function is only effective when the firewall is activated.

Console path:

Setup > **IP-Router** > **N-N-NAT**

2.8.20 Load balancer

This menu contains the configuration of load balancing for your IP router.

Console path:

Setup > **IP-Router**

2.8.20.1 Yes

This is where you can set parameters for load balancing. Load balancing can be used if your provider does not offer true channel bundling. At least one virtual connection must be specified in the load balancing table for this. The maximum number of remote sites that can be bundled depends on how many DSL ports are available for the type of device used.

Console path:

Setup > **IP-Router** > **Load-Balancer**

Possible values:

Yes
No

Default:

No

2.8.20.2 Bundle peers

If your Internet provider offers true channel bundling, it is possible for multiple connections to be combined with the help of load balancing.

Console path:

Setup > **IP-Router** > **Load-Balancer**

Possible values:

Yes
No

Default:

No

2.8.20.2.1 Peer

Unique name for a virtual load-balancing remote site. This remote site can then be used in the routing table.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

2.8.20.2.2 Bundle-Peer-1

Name of a previously configured remote site to which the others are to be bundled.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

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

Default:

empty

2.8.20.2.3 Bundle-Peer-2

Name of a previously configured remote site to which the others are to be bundled.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

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

Default:

empty

2.8.20.2.4 Bundle-Peer-3

Name of a previously configured remote site to which the others are to be bundled.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

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

Default:

empty

2.8.20.2.5 Bundle-Peer-4

Name of a previously configured remote site to which the others are to be bundled.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

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

Default:

empty

2.8.20.2.10 Client binding

Here you enable or disable the client binding for each load balancer.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

Yes

Client binding is enabled.

No

Client binding is disabled.

Default:

No

2.8.20.2.11 IPv4-Masq.

This menu item contains the settings for IPv4 masquerading in the load balancer.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

Auto

Adopts the masking option for each individual line from the routing table.

No

Deactivates NAT on all remote sites in the load balancer.

On

Activates NAT on all remote sites in the load balancer

intranet

Enables NAT for INTRANET type networks. The DMZ is not masked.

Default:

Auto

2.8.20.2.13 LB-Policy

Defines the Dynamic Path Selection Policy used for this firewall rule. This can either be one of the predefined ones from *2.8.20.4 Predefined-Selectors* on page 259 or one of the self-generated ones under *2.110.4.16 Policies* on page 1883.

The policy mentioned here is used as a fallback policy if no policy or the DEFAULT policy (see *2.8.20.4 Predefined-Selectors* on page 259) is entered in the firewall or the command line ping and applies to sessions that send via this load balancer.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

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

Default:

empty

2.8.20.3 Client binding

In this menu, you can configure the client binding.

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, this would limit all of the traffic to that server to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports

only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Console path:

Setup > **IP-Router** > **Load-Balancer**

2.8.20.3.1 Protocols

In this table, you specify the protocols and the associated ports for monitoring by the client binding.

The table already contains the default entries

- HTTPS
- HTTP
- ANY

Console path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

2.8.20.3.1.1 Name

Enter a descriptive name for this entry.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

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

Default:

empty

2.8.20.3.1.2 Protocol

Select the IP protocol number.

Learn more about IP protocol numbers in the *online database* of the IANA.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Max. 3 characters from `[0-255]`

Special values:

0

All protocols

Default:

0

2.8.20.3.1.3 Port

Select the port.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Max. 5 characters from `[0-65535]`

Special values:

0

All ports

Default:

0

2.8.20.3.1.4 Operating

Here you enable or disable the client binding for this entry.

Console path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Yes

Enables the entry

No

Disables the entry

Default:

Yes

2.8.20.3.2 Balance seconds

To prevent data from flowing through this main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

Console path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Possible values:

Max. 3 characters from `[0-999]`

Special values:

0

The timer is deactivated. All sessions are bound to the existing Internet connection.

Default:

10

2.8.20.3.3 Binding minutes

Specify the time in minutes for the binding entries to be valid for a client.

Console path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Possible values:

Max. 3 characters from `[0-999]`

Special values:

0

Default:

30

2.8.20.4 Predefined-Selectors

Here you will find some load balancer policies predefined by LCOS that can be used under *2.8.10.2.16 LB-Policy* on page 232 or *2.70.5.2.12 LB-Policy* on page 1592.

Note: This function only has an effect on routed data traffic. All internal services of the LANCOM router only use the ROUND-ROBIN policy.

Console path:

Setup > **IP-Router** > **Load-Balancer**

Possible values:

DEFAULT

This load balancer policy always has the same effect as not specifying a policy or leaving the LB-Policy column empty. In the firewall and in the command line ping, it triggers a fallback to the policy from table *2.8.20.2.13 LB-Policy* on page 256. In table *2.8.20.2.13 LB-Policy* on page 256, it triggers a fallback to the TRAFFIC selector.

TRAFFIC

This policy identifies the underlying physical connection for each channel and retrieves its absolute Rx load and Tx load from the columns Rx/s-average and Tx/s-average in **Status** > **WAN** > **Throughput**. If the physical bandwidth is known for all these physical connections (typically for wired connections but not for mobile networks), it calculates the relative loads by dividing the absolute loads by the respective bandwidth. Otherwise, it continues to work with the absolute loads. In the next step, it selects the larger value between the Rx and Tx loads. It then selects the channel with the lowest load.

BANDWIDTH

The load balancer policy BANDWIDTH selects a channel randomly. If the bandwidth is known for all underlying physical connections, the probability of selecting a particular channel is proportional to its bandwidth, i.e., a 50 Mbps channel is selected five times more often than a 10 Mbps channel. Otherwise, if at least one bandwidth is unknown, the channel is selected uniformly at random.

ROUND-ROBIN

The load balancer policy ROUND-ROBIN selects the channels in turn.

MOST-USED

With this policy, the load balancer selects the channel that currently has the most firewall sessions (regardless of whether in the send or receive direction and regardless of whether IPv4 or IPv6). This policy only makes sense as a counterpart to Dynamic Path Selection, i.e. if a branch device on the load balancer uses Dynamic Path Selection, then the head office should use MOST-USED on its associated load balancer. This effectively means that the head office adapts to the Dynamic Path Selection decisions of the branch office without the branch office having to explicitly communicate its decision to the head office.

2.8.23 Tag table

The tag table enables inbound data packets to be directly assigned with an interface tag that depends on the remote site.

Console path:

Setup > **IP-Router**

2.8.23.1 Peer

Name of the remote site whose packets are to be given interface tags when received.

Multiple remote sites can be configured in one entry by using "*" as a place holder. If, for example, several remote sites (RAS users) of a company are to be tagged, all appropriate remote sites can be given a name with the prefix "Company1_". To configure all of the remote sites, just one entry with remote site "Company1_*" can be included in the tag table.

Console path:

Setup > **IP-Router** > **Tag-Table**

2.8.23.2 Rtg-Tag

This interface tag is assigned to the inbound packets of the remote site.

Console path:

Setup > **IP-Router** > **Tag-Table**

Possible values:

0 … 65535

Default:

0

2.8.23.3 Start-WAN-Pool

The start WAN pool represents the beginning of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Console path:

Setup > **IP-Router** > **Tag-Table**

Possible values:

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

Default:

0.0.0.0

2.8.23.4 Ende-WAN-Pool

The end WAN pool represents the end of the address pool for the remote site or group of remote sites (when using placeholders to specify remote site). When RAS users dial in, the remote site is assigned an address from the address pool defined here.

Console path:

Setup > **IP-Router** > **Tag-Table**

Possible values:

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

Default:

0.0.0.0

Special values:

If the pool is empty (start and end addresses are 0.0.0.0), the global pool is used.

2.8.23.5 DNS-Default

Using this entry you configure the address that the remote station is given as its DNS server.

If the specified value is `0.0.0.0`, your device assigns the DNS server that is configured in the setup menu under **TCP-IP/DNS-Default**. If `0.0.0.0` is also entered there, your device assigns itself as the DNS server.

Console path:

Setup > **IP-Router** > **Tag-Table**

Possible values:

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

Default:

0.0.0.0

2.8.23.6 DNS-Backup

Using this entry you configure the address that the remote station is assigned as an alternate DNS server.

If the specified value is `0.0.0.0`, your device assigns the alternate DNS server that is configured in the setup menu under **TCP-IP/DNS-Backup**.

Console path:

Setup > **IP-Router** > **Tag-Table**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.8.24 ICMP

The ICMPv4 response rate limiting is configured here.

Rate limiting applies only to ICMP error messages and redirects.

- The rate limit applies to all interfaces.
- There is only one entry, **DEFAULT**.

Console path:

Setup > **IP-Router**

2.8.24.1 Interface name

Contains the name of the interface for which the entry was configured.

Console path:

Setup > **IP-Router** > **ICMP**

Possible values:

DEFAULT

Default:

DEFAULT

2.8.24.2 Max. size

Sets the maximum size of the token bucket.

In **packet** mode this is the number of packets, whereas in the **bandwidth** mode this is kbps.

Console path:

Setup > **IP-Router** > **ICMP**

Possible values:

0 … 65535

2.8.24.3 Refresh amount

Specifies the number of tokens added to the bucket in each interval before it is completely full.

Console path:

Setup > **IP-Router** > **ICMP**

Possible values:

0 … 65535

2.8.24.4 Interval

Sets the length of the interval in ms.

Console path:

Setup > **IP-Router** > **ICMP**

Possible values:

0 … 65535

2.8.24.5 Mode

Specifies the mode of the limitation.

Console path:

Setup > **IP-Router** > **ICMP**

Possible values:

Bandwidth

Each packet to be sent is checked for whether the number of tokens in the bucket exceeds the size of the packet in kbit. If this is the case, the packet is sent and the corresponding number of tokens is removed from the bucket. Otherwise the packet is not sent.

Packets

Each packet to be sent is checked for whether at least one token is currently available in the token bucket. If this is the case, the packet is sent and a token is removed from the bucket. Otherwise the packet is not sent.

Disabled

No limitation, the packets are always sent.

2.9 SNMP

This menu contains the configuration of SNMP.

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 IP traps table, enter the IP addresses of those computers where the SNMP managers are installed.

Console path:

Setup > **SNMP**

Possible values:

Yes
No

Default:

No

2.9.3 Administrator

Name of the device administrator. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.4 Location

Location information for this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.5 Register-Monitor

This action allows SNMP agents to log in to the device in order to subsequently receive SNMP traps. The command is specified together with the IP address, the port and the MAC address of the SNMP agent. All three values can be replaced with the wildcard *, in which case the device ascertains the values from the packets received from the SNMP agent.

A LANmonitor need not be explicitly logged in to the device. LANmonitor automatically transmits the login information to the device when scanning for new devices.

Console path:

Setup > **SNMP**

Possible values:

<IP-Address|*>:<Port|*> <MAC-Address|*> <W>

<W> at the end of the command is necessary if registration is to be effected over a wireless LAN connection.

2.9.6 Delete monitor

This action allows registered SNMP agents to be removed from the monitor list. The command is specified together with the IP address and the port of the SNMP agent. All three values can be replaced with the wildcard "*", in which case the device ascertains the values from the packets received from the SNMP agent.

Console path:

Setup > **SNMP**

Possible values:

<IP-Address|*>:<Port|*>

2.9.11 Comment-1

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.12 Comment-2

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.13 Comment-3

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.14 Comment-4

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.16 Comment-5

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.17 Comment-6

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.18 Comment-7

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.19 Comment-8

Comment on this device. For display purposes only.

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.20 Full host MIB

Please select whether a full host MIB is used for the device.

Console path:

Setup > **SNMP** > **Full-Host-MIB**

Possible values:

Yes
No

Default:

No

2.9.21 Port

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

Console path:

Setup > **SNMP**

Possible values:

0 … 65535

Default:

161

2.9.23 Public-Comment-1

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.24 Public-Comment-2

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.25 Public-Comment-3

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

2.9.26 Public-Comment-4

Console path:

Setup > **SNMP**

Possible values:

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

Default:

empty

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. By default, the configuration is set up for SNMP access via LANmonitor.

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 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:

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

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
Down

Default:

Active

2.9.29 Access

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** > **Access**

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** > **Access**

Possible values:

Any
Any model is accepted.

SNMPv1
SNMPv1 is used.

SNMPv2
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** > **Access**

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** > **SNMPv3-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** > **Access**

Possible values:

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

Default:

empty

2.9.29.9 Status

Activates or deactivates this entry.

Console path:

Setup > **SNMP** > **Access**

Possible values:

Active
Down

Default:

Active

2.9.29.10 Min-Security-Level

Specify the minimum security level for access and data transfer.

Console path:

Setup > **SNMP** > **Access**

Possible values:

NoAuth-NoPriv

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

Auth-NoPriv

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

Auth-Priv

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

Default:

Auth-Priv

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

2.9.30.2 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 are taken from the device MIB, which you can download with WEBconfig under **Extras** > **Get Device SNMP MIB**.

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
Down

Default:

Active

2.9.32 Users

This menu contains the user configuration.

Console path:

Setup > **SNMP**

2.9.32.2 User name

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).

Default:

HMAC-SHA

2.9.32.6 Authentication-Password

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

Console path:

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

Possible values:

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

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.

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)

Default:

AES128

2.9.32.9 Privacy-Password

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

Console path:

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

Possible values:

Max. 128 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
Down

Default:

Active

2.9.32.14 Authentication-Key

Encrypted authentication password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 384.

Console path:

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

Possible values:

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

Default:

empty

2.9.32.15 Privacy-Key

Encrypted privacy password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 384.

Console path:

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

Possible values:

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

Default:

empty

2.9.34 Target-Address

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 Target-Address-Name

Specify the target address name here.

Console path:

Setup > **SNMP** > **Target-Address**

Possible values:

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

Default:

empty

2.9.34.3 Target-Transport-Address

The transport address describes the IP address and port number of an SNMP trap receiver and is specified in the syntax <IP address>:<port> (for example, 128.1.2.3:162). UDP port 162 is used for SNMP traps.

Console path:

Setup > **SNMP** > **Target-Address**

Possible values:

Max. 32 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-Address**

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-Address**

Possible values:

Active
Inactive

Default:

Active

2.9.34.10 Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

Console path:

Setup > **SNMP** > **Target-Address**

Possible values:

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

Default:

empty

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:

SNMPv1
SNMPv2
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 trap.

Console path:

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

Possible values:

NoAuth-NoPriv

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.

Auth-NoPriv

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

Auth-Priv

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

Default:

NoAuth-NoPriv

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:

SNMPv1

SNMPv2

SNMPv3

2.9.38 Allow admins

Enable this option if registered administrators should also have access via SNMPv3.

Console path:

Setup > **SNMP**

Possible values:

No
Yes

Default:

Yes

2.9.39 SNMPv3-Admin-Authentication

Sets the authorization method for administrators.

This value cannot be modified.

Console path:

Setup > **SNMP**

Possible values:

AUTH-HMAC-SHA

Default:

AUTH-HMAC-SHA

2.9.40 SNMPv3-Admin-Privacy

Specifies the encryption settings for administrators.

This value cannot be modified.

Console path:

Setup > **SNMP**

Possible values:

AES256

Default:

AES256

2.9.41 Operating

This entry enables or disables SNMP traps. Clear the checkbox to disable SNMP traps.

Console path:

Setup > **SNMP**

Possible values:

No
Yes

Default:

Yes

2.9.42 Filter

Certain SNMP traps or even large numbers of SNMP traps can be unwanted on the receiving servers. For this reason, you can add an SNMP filter list that allows you to selectively pass or withhold SNMP traps based on their manufacturer-specific OIDs or the OIDs contained in the variable bindings.

Traps for the user “root” cannot be filtered. Filtering requires the use of a separate SNMP user.

Console path:

Setup > **SNMP**

2.9.42.1 Index

The position of this entry in the filter list. The list is checked from the smallest to the largest value until the first hit.

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Max. 4 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.9.42.2 View-Name

Enter the name of a view under **Setup** > **SNMP** > **Filters** > **View-Name** that this filter rule should apply to. If access in the value **Setup** > **SNMP** > **Filters** > **Type** is set to "Included" for this view, the corresponding traps can be prevented with the **filter action** "Prohibit" by means of a corresponding filter rule. However, if the corresponding access is set to "Excluded", the filter action "Allow" will continue to send the messages as an exception. Since the views can contain multiple entries of the same name with different access settings, it must be possible to set the filter action irrespective of the value set for **Setup** > **SNMP** > **Filters** > **Type**.

Console path:

Setup > **SNMP** > **Filter**

Possible values:

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

2.9.42.3 Spec.-TrapID

Specifies a certain trap ID that can contain wildcards and ranges. An empty entry applies to all specific trap IDs of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with "1.2.3".
1.*.3	Applies to all OIDs that start with "1", then contain any value, and then continue with "3".
1.2-3.4	Applies to all OIDs that start with "1", continue with a number ranging from "2 to 3", and then a "4".
1.2.3-4,7-8	Applies to all OIDs that start with "1.2" and continue with a number ranging from "3 to 4" or "7 to 8".

Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

A LANCOM device maps the generic trap OIDs of the SNMP protocol to certain vendor-specific OIDs:

Name	Generic OID	OID at LANCOM
coldStart	0	1.3.6.1.6.3.1.1.5.1
warmStart	1	1.3.6.1.6.3.1.1.5.2
linkDown	2	1.3.6.1.6.3.1.1.5.3
linkUp	3	1.3.6.1.6.3.1.1.5.4
authenticationFailure	4	1.3.6.1.6.3.1.1.5.5

Name	Generic OID	OID at LANCOM
egpNeighborLoss	5	1.3.6.1.6.3.1.1.5.6

Console path:

Setup > **SNMP** > **Filter**

Possible values:

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

2.9.42.4 Var.BindingID

Specifies an OID that must be in the trap's variable bindings, which in turn may contain wildcards and ranges. An empty entry applies to all variable bindings of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with "1.2.3".
1.*.3	Applies to all OIDs that start with "1", then contain any value, and then continue with "3".
1.2-3.4	Applies to all OIDs that start with "1", continue with a number ranging from "2 to 3", and then a "4".
1.2.3-4,7-8	Applies to all OIDs that start with "1.2" and continue with a number ranging from "3 to 4" or "7 to 8".

Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

Console path:

Setup > **SNMP** > **Filter**

Possible values:

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

2.9.42.5 Filter-Action

In case of a match with the set OID, you can either "Allow" the trap to send it, or "Deny" it so that it is discarded.

Console path:

Setup > **SNMP** > **Filter**

Possible values:

Allow
Deny

2.11.93 Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for the SNMPv3 passwords:

- The length of the password must be at least 16 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

Please note that SNMPv3 only uses passwords, when in the table **Setup** > **SNMP** > **Users** neither **Authentication-Protocol** nor **Privacy-Protocol** is set to **None**.

Console path:

Setup > **Config**

Possible values:

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

No

2.11.89.1 Keep-Cleartext

As of LCOS 10.40 an algorithm is used to store the password of SNMP users in encrypted form as a hash value. Specify here whether the cleartext password is also retained.

Console path:

Setup > **Config**

Possible values:

Yes

The passwords of SNMP users are internally also stored in cleartext.

If you wish to retain the option of downgrading the firmware to an LCOS version earlier than 10.40, this option must be set.

No

The passwords of SNMP users are internally stored in hashed form only.

Default:

Yes

2.10 DHCP

This menu contains the DHCP settings.

Console path:

Setup

2.10.6 Max. lease time minutes

When a client requests an IP address from a DHCP server, it can also ask for a lease period for the address. This values governs the maximum length of lease that the client may request.

Console path:

Setup > **DHCP**

Possible values:

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

Default:

6000

2.10.7 Default lease time minutes

When a client requests an address without asking for a specific lease period, the address will be assigned the value set here as lease.

Console path:

Setup > **DHCP**

Possible values:

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

Default:

500

Special values:

0

A default lease time of 2 minutes is used.

2.10.8 DHCP table

The DHCP table provides an overview of the IP addresses used in the IP networks. The DHCP table is purely a status table where no parameters can be configured.

Console path:

Setup > **DHCP**

2.10.8.1 IP address

IP address used by the client.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.2 MAC address

The client's MAC address.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.3 Timeout

Lease for the address assignment in minutes.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.4 Host name

Name of the client, if it was possible to determine this.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.5 Type

The "Type" field indicates how the address was assigned.

Console path:

Setup > **DHCP** > **DHCP-Table**

Possible values:

new

The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.

unkn.

When the server checked if the address was unique, it was found that the address had already been assigned to another client. Unfortunately, the DHCP server does not have any way of obtaining further information about this client.

stat.

A client has informed the DHCP server that it has a fixed IP address. This address may not be used for any other clients in the network.

dyn.

The DHCP server has assigned an address to the client.

2.10.8.7 Ethernet port

Physical interface connecting the client to the device.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.8 VLAN-ID

The VLAN ID used by the client.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.9 Network name

Name of the IP network where the client is located.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.10 LAN Ifc

The LAN interface that this entry refers to.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.8.11 Assignment

This column shows the time stamp (date and time in the format "dd.mm.yyyy hh:mm:ss") when the DHCP assignment for the specified IP address was made.

Console path:

Setup > **DHCP** > **DHCP-Table**

2.10.9 Hosts

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. For this, the workstation's MAC address is entered in the hosts table.

Console path:

Setup > **DHCP**

2.10.9.1 MAC address

Enter the MAC address of the workstation to which an IP address is to be assigned.

Console path:

Setup > **DHCP** > **Hosts**

2.10.9.2 IP address

Enter the client IP address that is to be assigned to the client.

Console path:

Setup > **DHCP** > **Hosts**

2.10.9.3 Host name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Console path:

Setup > **DHCP** > **Hosts**

Possible values:

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

Default:

empty

2.10.9.4 Image alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

Console path:

Setup > **DHCP** > **Hosts**

Possible values:

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

Default:

empty

2.10.9.5 Network name

Enter the name of a configured IP network here. Only if a requesting client is located in this IP network will it be assigned the relevant IP address defined for the MAC address.

If the requesting client is located in an IP network for which there is no corresponding entry in the hosts table, the client will be assigned an IP address from the address pool of the appropriate IP network.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

Console path:

Setup > **DHCP** > **Hosts**

Possible values:

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

Default:

empty

Special values:

empty

The IP address will be assigned if the IP address defined in this field belongs to the range of addresses for the IP network where the requesting client is located.

2.10.10 Alias-List

The alias list defines the names for the boot images that are used to reference the images in the hosts table.

Console path:

Setup > **DHCP**

2.10.10.1 Image alias

Enter any name you wish for this boot image. This name is used when you assign a boot image to a particular client in the station list.

Console path:

Setup > **DHCP** > **Alias-List**

Possible values:

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

Default:

empty

2.10.10.2 Image file

Enter the name of the file on the server containing the boot image.

Console path:

Setup > **DHCP** > **Alias-List**

Possible values:

Max. 60 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.10.10.3 Image server

Enter the IP address of the server that provides the boot image.

Console path:

Setup > **DHCP** > **Alias-List**

2.10.18 Ports

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

Console path:

Setup > **DHCP**

2.10.18.2 Port

Select the logical interface for which the DHCP server should be enabled or disabled.

Console path:

Setup > **DHCP** > **Ports**

Possible values:

Select from the list of logical devices in this device, e.g. LAN-1, WLAN-1, P2P-1-1 etc.

2.10.18.3 Port

Enables or disables the DHCP server for the selected logical interface.

Console path:

Setup > **DHCP** > **Ports**

Possible values:

Yes
No

Default:

Yes

2.10.20 Network list

DHCP settings for the IP networks are defined in this table. If multiple DHCP servers are active in a network, the stations "divide" themselves equally between them. However, the DNS server in devices can only properly resolve the name of the station which was assigned the address information by the DHCP server. In order for the DNS server to be able to resolve the names of other DHCP servers, these can be operated in a cluster. In this operating mode, the DHCP server monitors all DHCP negotiations in the network. It additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster.

A DHCP server's operation in the cluster can be activated or deactivated for each individual ARF network with the associated DHCP settings.

Console path:

Setup > **DHCP**

2.10.20.1 Network name

The name of the network which the DHCP server settings apply to.

Console path:

Setup > **DHCP**

Possible values:

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

Default:

empty

2.10.20.2 Start address pool

The first IP address in the pool available to the clients. If no address is entered here the DHCP server takes the first available IP address from the network (as determined by network address and netmask).

Console path:

Setup > **DHCP** > **Network-List**

2.10.20.3 End address pool

The last IP address in the pool available to the clients. If no address is entered here the DHCP server takes the last available IP address from the network (as determined by network address and netmask).

Console path:

Setup > **DHCP** > **Network-List**

2.10.20.4 Netmask

Corresponding netmask for the address pool available to the clients. If no address is entered here the DHCP server uses the netmask from the corresponding network.

Console path:

Setup > **DHCP** > **Network-List**

2.10.20.5 Broadcast address

As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address is entered into the DHCP module. With the default value, the broadcast address is found automatically.

We recommend that only experienced network specialists change the presetting for the broadcast address. Errors in the configuration can lead to the establishment of undesired and costly connections.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.6 Gateway address

As standard, the DHCP server issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can also be transmitted if a corresponding address is entered here.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.7 DNS-Default

IP address of the DNS name server that the requesting workstation should use.

If no default or backup DNS server is defined, the device will assign the requesting workstation its own IP address in the relevant ARF network as (primary) DNS server.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.8 DNS-Backup

IP address of the backup DNS name server. The workstation will use this DNS server if the first DNS server fails

If no default or backup DNS server is defined, the device will assign the requesting workstation its own IP address in the relevant ARF network as (primary) DNS server.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.11 Operating

DHCP server operating mode in this network. Depending on the operating mode, the DHCP server can enable/disable itself. The DHCP statistics show whether the DHCP server is enabled.

Only use the setting "Yes" if you are certain that no other DHCP server is active in the LAN.

Only use the "client mode" setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

No

DHCP server is permanently switched off.

Yes

DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked. If the configuration is correct then the device starts operating as a DHCP server in the network. Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be deactivated. Only use this setting if you are certain that no other DHCP server is active in the LAN.

Auto

With this setting, the device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress. If another DHCP server is discovered the device switches its own DHCP server off. If the LANCOM is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally. If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the device will be disabled.

Relay

The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests, but forwards them to a central DHCP server elsewhere in the network (DHCP relay agent mode).

Client

The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Only use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

Stateless-relay

The device accepts requests from DHCP clients in the local network. However, the device does not answer these requests itself, but forwards them to a central DHCP server in another network section (DHCP relay agent mode).

The Stateless Relay Agent does not modify DHCP packets from the client to the server and back. In particular, unlike the Relay Agent, the DHCP server identifier is not modified.

Default:

No

2.10.20.12 Broadcast bit

This setting decides whether the broadcast bit from clients is to be checked. If the bit is not checked then all DHCP messages are sent as broadcasts.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes
No

Default:

No

2.10.20.13 Master server

This is where the IP address for the upstream DHCP server is entered where DHCP requests are forwarded when the mode "Relay requests" is selected for the network.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.14 Cache

This option allows the responses from the superordinate DHCP server to be stored in the device. Subsequent requests can then be answered by the device itself. This option is useful if the superordinate DHCP server can only be reached via a connection which incurs costs.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes
No

Default:

No

2.10.20.15 Adaptation

This option allows the responses from the superordinate DHCP server to be adapted to the local network. When activated, the device adapts the responses from the superordinate DHCP server by replacing the following entries with its own address (or local configured addresses):

Gateway

Netmask

Broadcast address

DNS server

Server ID

This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes
No

Default:

No

2.10.20.16 Cluster

This setting defines whether the DHCP server for this ARF network is to be operated separately or in the cluster.

If the lease time for the information supplied by DHCP expires, the station requests a renewal from the DHCP server which supplied the original information. If the original DHCP server does not respond, the station then emits its rebinding request as a broadcast to all available DHCP servers. DHCP servers in a cluster ignore renew requests, which forces a rebinding. The resulting broadcast is used by all of the DHCP servers to update their entries for the station. The only DHCP server to answer the rebind request is the one with which the station was originally registered. If a station repeats its rebind request, the all DHCP servers in the cluster assume that the original DHCP server is no longer active in the cluster, and they respond to the request. The responses received by the station will have the same IP address, but the gateway and DNS server addresses may differ. From these

responses, the station selects a new DHCP server to connect with, and it updates its gateway and DNS server (and other relevant parameters) accordingly.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes

With cluster mode activated, the DHCP server monitors all of the ongoing DHCP negotiations in the network, and it additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster. These stations are flagged as "cache" in the DHCP table.

No

The DHCP server manages information only for the stations connected to it.

Default:

No

2.10.20.17 2nd master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode "Relay requests" is selected for the network.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.18 3rd master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode "Relay requests" is selected for the network.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.19 4th master server

This is where the IP address for an alternative DHCP server is entered where DHCP requests are forwarded when the mode "Relay requests" is selected for the network.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 16 characters from `[0-9].`

Default:

0.0.0.0

2.10.20.20 Max.-Lease

In addition to the global maximum lease time configured under **Setup** > **DHCP**, it is possible to configure a maximum lease time specifically for this DHCP network only.

Here you specify the maximum lease time that a client may request.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

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

Default:

0

Special values:

0

The DHCP server uses the value *2.10.6 Max. lease time minutes* on page 290).

2.10.20.21 Def.-Lease

In addition to the global default lease time configured under **Setup** > **DHCP**, it is possible to configure a default lease time specifically for this DHCP network only.

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

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

Default:

0

Special values:

0

The DHCP server uses the value *2.10.7 Default lease time minutes* on page 290).

2.10.20.22 Loopback address

Here you assign a loopback address to a relay agent. The loopback address (the name of an ARF network, named loopback address) is used to forward client messages.

Console path:

Setup > **DHCP**

Possible values:

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

Default:

empty

2.10.20.23 Suppress-ARP-check

Before the DHCP server assigns an IP address, an ARP request is usually used to check whether the address has been assigned already. If there is no response to the ARP request within 3 seconds, the assignment goes ahead. This query is especially useful when computers are booting in normal networks that use fixed IP addresses. In a Public Spot network where, for example, a smartphone has to recognize that there is no Internet connection in order to display the login popup, this ARP request leads to an unnecessary delay. For scenarios such as this, this check can be disabled here.

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes

Do not carry out check by ARP request.

No

Perform check by ARP request.

Default:

No

2.10.23 RADIUS accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a `RADIUS accounting start` to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a `RADIUS accounting stop`. In between these

two events, the DHCP server regularly sends the RADIUS server a `RADIUS accounting interim update` in a configurable interval.

This menu contains the settings for the DHCP lease RADIUS accounting.

Console path:

Setup > **DHCP**

2.10.23.1 Operating

Enables or disables the RADIUS accounting on this DHCP network.

Console path:

Setup > **DHCP** > **RADIUS-Accounting**

Possible values:

No

RADIUS accounting is disabled for this network.

Yes

RADIUS accounting is enabled for this network.

Default:

No

2.10.23.2 Interim Interval

Here you specify the time interval in seconds after which the DHCP server sends a `RADIUS interim update` to the accounting server.

Console path:

Setup > **DHCP** > **RADIUS-Accounting**

Possible values:

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

2.10.23.20 Network list

This table contains the IP networks for the RADIUS accounting.

Console path:

Setup > **DHCP** > **RADIUS-Accounting**

2.10.23.20.1 Network name

Contains the name of the network.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.2 Server host name

Enter the host name of the RADIUS accounting server here.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.3 Accnt.-Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port “1813”.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

1813

2.10.23.20.4 Secret

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.5 Loopback address

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.6 Protocol

Use this entry to specify the protocol used to communicate with the RADIUS accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.10.23.20.7 Attribute-Values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.12 Backup server hostname

Enter the host name of the backup server here.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.13 Backup-Accnt.-Port

Here you enter the backup port used by the backup RADIUS accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

0

2.10.23.20.14 Backup secret

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.15 Backup-Loopback-Address

Specify a loopback address for the backup RADIUS accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.23.20.16 Backup-Protocol

Use this entry to specify the protocol used to communicate with the backup RADIUS accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.10.23.20.17 Backup attribute values

Here you specify the attribute values for the backup RADIUS accounting server.

Console path:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Possible values:

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

Default:

empty

2.10.25 LMC options

In this table, you configure the cloud parameters for the LMC (LANCOM Management Cloud).

Console path:

Setup > **DHCP**

2.10.25.1 Network name

Here you specify the network to which the device delivers the LMC domain via DHCP option 43.

Console path:

Setup > **DHCP** > **LMC-Options**

Possible values:

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

Default:

empty

2.10.25.6 LMC domain

Enter the domain name for the LANCOM Management Cloud 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 > **DHCP** > **LMC-Options**

Possible values:

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

Default:

empty

2.10.25.7 Rollout-Project-ID

Enter the project ID of the LANCOM Management Cloud (LMC) to be delivered to the devices via DHCP. At the first connection to the LMC the device will be assigned accordingly.

Console path:

Setup > **DHCP** > **LMC-Options**

Possible values:

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

Default:

empty

2.10.25.8 Rollout-Location-ID

Enter the location ID of the LANCOM Management Cloud (LMC) to be delivered to the devices via DHCP. At the first connection to the LMC the device will be assigned accordingly.

Console path:

Setup > **DHCP** > **LMC-Options**

Possible values:

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

Default:

empty

2.10.26 Additional options

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows e.g. the type of device. This table allows additional options for DHCP operations to be defined.

Console path:

Setup > **DHCP**

2.10.26.1 Option number

Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP.

You can find a list of all DHCP options in RFC 2132 – "DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.26.2 Network name

Name from the list of defined IP networks for the IP network where this DHCP option is to be used.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

Possible values:

Special values:

empty

If no network name is specified the DHCP option defined in this entry will be used in all IP networks.

2.10.26.3 Option value

This field defines the contents of the DHCP option. IP addresses are normally specified using the conventional IPv4 notation, e.g. `123.123.123.100`. Integer tapes are usually entered in decimal digits and string types as simple text. Multiple values in a single field are separated with commas, e.g.`123.123.123.100, 123.123.123.200`.

The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.26.4 Option type

This value depends on the respective option. For option "35" according to RFC 1232, e.g. the ARP cache time is defined as follows:

ARP Cache Timeout Option This option specifies the time out in seconds for ARP cache entries. The time is specified as a 32-bit unsigned integer. The code for this option is 35, and its length is 4.

Code	Len	Time			
35	4	t1	t2	t3	t4

This description tells you that this the type "32-bit integer" is used for this option.

You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

String
Integer8
Integer16
Integer32
IP address

Default:

String

2.10.26.5 Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.26.6 Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. For example, DHCP requests from LANCOM devices always contain the string "LANCOM" in the vendor-class ID, which is supplemented by the exact device type, if required. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.26.7 User class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. This usually allows the manufacturer or even the specific device class of the client to be identified. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.26.8 Append-Sub-Option

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

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

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

Console path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Yes

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

No

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

2.10.27 Relay-Info-List

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. To this end, the switches provide the "Circuit ID" of the respective ports. Each port is then assigned exactly one IP address, host name and a boot image. The latter works analogous to the BOOTP table.

Console path:

Setup > **DHCP**

2.10.27.1 Circuit-ID

This is the storage location for the "Circuit ID" used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the "Circuit ID" is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires "negative" bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8}{2/8}{30/16}MES-3728
- {0x00/8}{0x02/8}{0x1e/16}MES-3728
- {00/8}{02/8}{036/16}MES-3728

Console path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

Max. 64 characters from `[A-F][a-f]x[0-9]{}/`

2.10.27.2 IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

Console path:

Setup > **DHCP** > **Relay-Info-List**

2.10.27.3 Host name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Console path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

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

Default:

empty

2.10.27.4 Image-alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

Console path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

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

Default:

empty

2.10.29 Echo client ID

According to the original DHCPv4 specification RFC 2131, the DHCPv4 server was not allowed to send client ID options in its response to clients. This occasionally gave rise to problems that were resolved with RFC 6842, the successor to RFC 2131. According to this update, the response from a DHCPv4 server must contain the client ID if the client sent this in its request. Since there may be older clients unable to cope with this changed behavior, you can re-enable the previous behavior here.

Console path:

Setup > **DHCP**

Possible values:

Yes

Compliant with RFC 6842.

No

Compliant with RFC 2131.

Default:

Yes

2.10.40 Client

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

Console path:

Setup > **DHCP**

2.10.40.2 User-Class-Identifier

The DHCP client in the device can supplement the transmitted DHCP requests with additional information to simplify the recognition of request within the network. The vendor class ID (DHCP option 60) shows the type of device. The vendor class ID is always transmitted. The user class ID (DHCP option 77) specifies a user-defined string. The user class ID is only transmitted when the user has configured a value.

Console path:

Setup > **DHCP** > **Client**

Possible values:

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

Default:

empty

2.10.40.3 Vendor class identifier

The vendor class ID (DHCP option 60) shows the type of device. The vendor class ID is always transmitted.

Console path:

Setup > **DHCP** > **Client**

Possible values:

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

Default:

empty

2.10.40.4 Accept-Gateway-and-Routes

This toggle controls the behavior of the DHCP client when it is assigned routes from the DHCP server via the "classless static routes option" (see *RFC 3442*) and also a default gateway via the "router option".

Console path:

Setup > **DHCP** > **Client**

Possible values:

Yes

The DHCP client accepts the assignment of default gateways even if routes are assigned at the same time.

No

The DHCP client accepts the assignment of default gateways only if **no** routes are assigned at the same time. This behavior corresponds to the RFC, but leads to problems with providers who do not comply with the RFC.

Default:

Yes

2.10.40.5 Additional options

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

Console path:

Setup > **DHCP** > **Client**

2.10.40.5.1 Interface

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

Console path:

Setup > **DHCP** > **Client** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.40.5.2 Option-Number

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

Console path:

Setup > **DHCP** > **Client** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.40.5.3 Option-Type

Specifies the type of the DHCP option.

Console path:

Setup > **DHCP** > **Client** > **Additional-Options**

Possible values:

String
Integer8
Integer16
Integer32
IP address

2.10.40.5.4 Option-Value

Specifies the content of the DHCP option

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

Console path:

Setup > **DHCP** > **Client** > **Additional-Options**

Possible values:

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

Default:

empty

2.10.40.5.5 Request-List

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

Console path:

Setup > **DHCP** > **Client** > **Additional-Options**

Possible values:

No
Yes

2.10.40.31 LAN-Client-ID-Type

This control influences how the Client-ID-Option is structured in DHCPDISCOVER and DHCPREQUEST messages from the DHCPv4 client on the LAN.

Console path:

Setup > **DHCP** > **Client**

Possible values:

MAC

The Client ID contains only the MAC address of the device. Before LCOS 10.70 the MAC address was always used automatically as the client ID without its own configuration option. When the firmware is updated, this value is retained.

DUID

Compliant to *RFC 4361*, the Client ID is formed as a DUID (DHCP Unique IDentifier) from the IAID and the MAC address of the device. This is the default on new installations as of LCOS 10.70.

Default:

DUID

2.10.40.32 WAN-Client-ID-Type

This control influences how the Client-ID-Option is structured in DHCPDISCOVER and DHCPREQUEST messages from the DHCPv4 client on the WAN.

Console path:

Setup > **DHCP** > **Client**

Possible values:

MAC

The Client ID contains only the MAC address of the device. Before LCOS 10.70 the MAC address was always used automatically as the client ID without its own configuration option. When the firmware is updated, this value is retained.

DUID

Compliant to *RFC 4361*, the Client ID is formed as a DUID (DHCP Unique IDentifier) from the IAID and the MAC address of the device. This is the default on new installations as of LCOS 10.70.

Default:

DUID

2.11 Config

Contains the general configuration settings.

Console path:

Setup

2.11.4 Maximum connections

The maximum number of simultaneous configuration connections to this device.

Console path:

Setup > **Config**

Possible values:

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

Default:

0

Special values:

0

This value switches the restriction off.

2.11.5 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. 2 characters from `[0-9]`

Default:

15

2.11.6 Language

Terminal mode is available in English or German. Devices are set with English as the default console language.

Console path:

Setup > **Config**

Possible values:

Deutsch
English

Keep in mind that the language of the commands should be the same as the language of the console, otherwise the commands will be ignored.

Default:

English

2.11.7 Login errors

In order to protect the configuration of your device against unauthorized access, the device can lock itself after repeated incorrect attempts to log in. Use this setting to specify the number of incorrect login attempts that are allowed before the device is locked.

Console path:

Setup > **Config**

Possible values:

Max. 16 characters from `[0-9]`

Default:

10

2.11.8 Lock minutes

In order to protect the configuration of your device against unauthorized access, the device can lock itself after repeated incorrect attempts to log in. Enter the period for which the lock is to be active for. Access to the device will only be possible after this period expires.

Console path:

Setup > **Config**

Possible values:

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

Default:

45

Special values:

0

The value "0" switches the lock off.

2.11.10 Display contrast

This item allows you to set the contrast for the display of the device.

Console path:

Setup > **Config**

Possible values:

C1 (low contrast) … C8 (high contrast)

Default:

C4

2.11.12 WLAN-authentication pages only

This setting gives you the option of restricting device access via the Public Spot interface to the Public Spot authentication pages only. All other configuration protocols are automatically blocked.

Public Spot access to a Public Spot network's configuration (WEBconfig) should always be prohibited for security reasons. We strongly recommend that you enable this setting for Public Spot scenarios!

Console path:

Setup > **Config**

Possible values:

No
Yes

Default:

No

2.11.13 TFTP client

Default values for the device configuration, firmware and/or a script can be used if the latest configurations, firmware versions and scripts are always stored under the same name in the same location. In this case, the simple commands LoadConfig, LoadFirmware and LoadScript can be used to load the relevant files.

Console path:

Setup > **Config**

2.11.13.1 Config address

Default path for configuration files when the parameter `-f` is not specified for LoadConfig commands.

The path is specified with the notation `//Server/Directory/File name`

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.13.2 Config file name

Default name of the configuration file when the parameter `-f` is not specified for "LoadConfig" commands.

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.13.3 Firmware address

Default path for firmware files when the parameter `-f` is not specified for "LoadFirmware" commands.

The path is specified with the notation `//Server/Directory/File name`

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.13.4 Firmware file name

Default name of the firmware file when the parameter `-f` is not specified for "LoadFirmware" commands.

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.13.5 Bytes per hashmark

Number of bytes used per hashmark.

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

max. 6 Zeichen aus `[0-9]`

Default:

8192

2.11.13.6 Script address

Default path for scripts when the parameter `-f` is not specified for "LoadScript" commands.

The path is specified with the notation `//Server/Directory/File name`

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.13.7 Script file name

Default name of the script when the parameter `-f` is not specified for "LoadScript" commands.

Console path:

Setup > **Config** > **TFTP-Client**

Possible values:

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

Default:

empty

2.11.15 Access table

Here you can set the access rights separately for each network and configuration protocol. You can also set limitations on the access to certain stations.

Console path:

Setup > **Config**

2.11.15.1 Ifc.

The interface that this entry refers to.

Console path:

Setup > **Config** > **Access-Table**

2.11.15.2 Telnet

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.3 TFTP

Use this option to set the access rights for configuring the device via the TFTP protocol (Trivial File Transfer Protocol). This protocol is required, for example, for configuration using the LANconfig application.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.4 HTTP

Use this option to set the access rights for configuring the device via the HTTP protocol (Hypertext Transfer Protocol). This protocol is required for configuring the device via the implemented web-based browser interface independent of the operating system.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.5 SNMP

Use this option to set the access rights for configuring the device via the SNMP protocol (SNMPv1 and SNMPv2). This protocol is required, for example, for configuring the device using the LANmonitor application.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

2.11.15.6 HTTPS

Use this option to set the access rights for configuring the device via the HTTPS protocol (Hypertext Transfer Protocol Secure or HTTP via SSL). This protocol is required for configuring the device via the implemented web-browser interface independent of the operating system.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.7 Telnet-SSL

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.8 SSH

Use this option to set the access rights for configuring the device via the TELNET/SSH protocol. This protocol is required for configuring the device securely via the implemented Telnet console from text-based systems independent of the operating system.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.15.9 SNMPv3

Use this option to set the access rights for configuring the device via the SNMP protocol (SNMPv3). This protocol is required, for example, for configuring the device using the LANmonitor application.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

2.11.15.10 Config Sync

Indicates whether a config sync is possible (restricted) via this interface.

Console path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

VPN-capable devices only.

Yes

Access is generally possible.

By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Default setting for the WAN interface.

Default:

Yes

No

2.11.16 Screen height

Specifies the maximum height of the screen in lines.

Console path:

Setup > **Config**

Possible values:

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

Default:

24

Special values:

0

The device automatically sets the optimum screen height during login.

2.11.17 Prompt

This value sets the prompt on the command line.

Console path:

Setup > **Config**

Possible values:

Max. 31 characters from `[a-z]%`

Default:

empty

Possible values:

%f

Starts a [Test] if you previously entered the command "flash no" on the command line. The command "flash no" activates the test mode for the configuration changes outlined below. When test mode is enabled, the device saves the changes to the configuration in RAM only. As the device's RAM is deleted during a reboot, all of the configuration changes made in test mode are lost. The [Test] display alerts the administrator about this potential loss of changes to the configuration.

%u

User name

%n

Device name

%p

Current path

%t

Current time

%o

Current operating time

2.11.18 LED test

Activates the test mode for the LEDs to test LED function in different colors.

Console path:

Setup > **Config**

Possible values:

Off

Switches all LEDs off.

Red

Switches all LEDs on that emit red.

Green

Switches all LEDs on that emit green.

Orange

Switches all LEDs on that emit orange.

No_Test:

Normal LED operating mode.

Default:

No_Test:

2.11.20 Cron table

CRON jobs are used to carry out recurring tasks on a device automatically at certain times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result if, for example, all devices try to establish a VPN connection at once. To avoid these effects, the CRON jobs can be set with a random delay time between 0 and 59 minutes.

Console path:

Setup > **Config**

2.11.20.1 Index

Index for this entry.

Console path:

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

Possible values:

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

Default:

empty

2.11.20.2 Minute

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Minute values range from 0 to 59.

Examples:

- /10 – Every 10 minutes
- 0,10,20,30,40,50 – Every 10 minutes
- 0-30/5 – Every 5 minutes within the first half-hour
- 0-59 – Every minute
- 25-30 – At minutes 25 through 30
- 25,26,27,28,29,30 – At minutes 25 through 30
- 55-5 – At minutes 55 through 5
- 55,56,57,58,59,0,1,2,3,4,5 – At minutes 55 through 5

Console path:

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

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

2.11.20.3 Hour

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Hour values range from 0 to 23.

Examples:

- /4 – Every 4 hours
- 0,4,8,12,16,20 – Every 4 hours
- 8-20/2 – Every 2 hours between 8 AM and 8 PM
- 0-23 – Every hour
- 13-16 – Between hours 13 and 16
- 13,14,15,16 – Between hours 13 and 16
- 22-1 – Between hours 22 and 1
- 22,23,0,1 – Between hours 22 and 1

Console path:

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

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

2.11.20.4 DayOfWeek

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Day-of-week values range from 0 (Sunday) to 6 (Saturday). For syntax examples, see Minute or Hour.

Console path:

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

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

2.11.20.5 Day

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Day values range from 1 to 31. For syntax examples, see Minute or Hour.

Console path:

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

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

2.11.20.6 Month

The value defines the time at which a command is to be executed. If no value is specified, it will not be included in the scheduling. A comma-separated list of values or a range can also be entered. A step size can be specified using /. If a range precedes the step size, it applies to the defined range. Month values range from 1 (January) to 12 (December). For syntax examples, see Minute or Hour.

Console path:

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

Possible values:

Max. 50 characters from `[0-9] ,-/`

Default:

empty

2.11.20.7 Command

The command to be executed or a comma-separated list of commands. Any command-line function can be executed.

Console path:

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

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.11.20.8 Basic

The time base field determines whether time control is based on real time or on the device's operating time.

Console path:

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

Possible values:

Real-Time

These rules evaluate all time/date information. Real-time based rules can be executed provided that the device has a time from a relevant source, e.g. via NTP.

Operation-Time

These rules only evaluate the minutes and hours since the last time the device was started.

Default:

Real-Time

2.11.20.9 Operating

Activates or deactivates the entry.

Console path:

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

Possible values:

Yes
No

Default:

Yes

2.11.20.10 Owner

An administrator defined in the device can be designated as owner of the CRON job. If an owner is specified, then the CRON job commands will be executed with the rights of the owner.

Console path:

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

Possible values:

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

Default:

empty

2.11.20.11 Variation

This specifies the maximum delay, from 0 to 65536 minutes, for the start of the CRON job after the set start time. The actual delay time is determined randomly and lies between 0 and the time entered here.

Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.

Console path:

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

Possible values:

0 … 65535 Seconds

Default:

0

Special values:

When set to zero, the CRON job is executed at precisely the defined time.

2.11.20.12 Comment

This parameter is used to leave a comment about the entry in the CRON table.

Console path:

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

Possible values:

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

Default:

empty

2.11.21 Admins

Here you can create additional administrator user accounts.

Only the root administrator can create or edit additional administrators. All other administrators are denied access to these settings. Neither read-only nor write access is possible via SNMP.

Console path:

Setup > **Config**

2.11.21.1 Administrator

Multiple administrators can be set up in the configuration of the device, each with different access rights. Up to 16 different administrators can be set up for a device.

Besides these administrators set up in the configuration, there is also the “root” administrator with the main password for the device. This administrator always has full rights and cannot be deleted or renamed. To log in as root administrator, enter the user name “root” in the login window or leave this field empty. As soon as a password is set for the “root” administrator in the device's configuration, WEBconfig will display the button Login that starts the login window. After entering the correct user name and password, the WEBconfig main menu will appear. This menu only displays the options that are available to the administrator who is currently logged in. If more than one administrator is set up in the admin table, the main menu features an additional button 'Change administrator' which allows other users to log in (with different rights, if applicable).

Only the root administrator can create or edit additional administrators.

Console path:

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

Possible values:

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

Default:

empty

2.11.21.2 Password

Password for this entry.

Console path:

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

Possible values:

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

Default:

empty

2.11.21.3 Function rights

Each administrator has "function rights" that determine personal access to certain functions such as the Setup Wizards. You assign these function rights when you create a new administrator.

If you create a new administrator via Telnet, the following hexadecimal values are available to you. By entering one or more of these values with **set** you set the function rights.

In WEBconfig you assign the function rights by selecting the appropriate check boxes in the menu shown below.

Console path:

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

Possible values:

0x00000001

The user can run the Basic Wizard.

0x00000002

The user can run the Security Wizard.

0x00000004

The user can run the Internet Wizard.

0x00000008

The user can run the Wizard for selecting Internet providers.

0x00000010

The user can run the RAS Wizard.

0x00000020

The user can run the LAN-LAN Coupling Wizard.

0x00000040

The user can set the date and time (also applies for Telnet and TFTP).

0x00000080

The user can search for additional devices.

0x00000100

The user can run the WLAN Link test (also applies for Telnet).

0x00000200

The user can run the a/b Wizard.

0x00000400

The user can run the WTP Assignment Wizard.

0x00000800

The user can run the Public Spot Wizard.

0x00001000

The user can run the WLAN Wizard.

0x00002000

The user can run the Rollout Wizard.

0x00004000

The user can run the Dynamic DNS Wizard.

0x00008000

The user can run the VoIP Call Manager Wizard.

0x00010000

The user can run the WLC Profile Wizard.

0x00020000

The user can use the integrated Telnet or SSH client.

0x00100000

The user can run the Public-Spot User management Wizard.

empty

Default:

2.11.21.4 Active

Activates or deactivates this function.

Console path:

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

Possible values:

Yes
No

Default:

Yes

2.11.21.5 Access rights

Access to the internal functions can be configured for each interface separately:

- ISDN administration access
- LAN
- Wireless LAN (WLAN)
- WAN (e.g. ISDN, DSL or ADSL)

Access to the network configuration can be further restricted so that, for example, configurations can only be edited from certain IP addresses or LANCAPI clients. Furthermore, the following internal functions can be switched on/off separately:

- LANconfig (TFTP)
- WEBconfig (HTTP/HTTPS)
- SNMP
- Terminal/Telnet

For devices supporting VPN, it is also possible for internal functions that operate over WAN interfaces to be restricted to VPN connections only.

Console path:

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

Possible values:

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

Default:

2.11.21.6 Encrypted-Password

Encrypted password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 384.

Console path:

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

Possible values:

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

Default:

empty

2.11.21.7 SNMP encrypted password

Encrypted SNMP password for this entry.

This password is automatically encrypted by the algorithm specified in *2.11.89.2 Crypto-Algorithm* on page 384.

Console path:

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

Possible values:

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

Default:

empty

2.11.23 Telnet port

This port is used for unencrypted configuration connections via Telnet.

Console path:

Setup > **Config**

Possible values:

Max. 10 characters from `0-9]`

Default:

23

2.11.27 Predef.-Admins

Here you will find the predefined administrator account for the device. This administrator account is used when no user name is defined when logging in.

Console path:

Setup > **Config**

2.11.27.1 Name

Enter the name of the predefined administrator account here.

Console path:

Setup > **Config** > **Predef.-Admins**

Possible values:

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

Default:

empty

2.11.28 SSH

This item manages the mechanisms used for SSH encryption. You can select which algorithms are supported in both server and client mode.

Console path:

Setup > **Config**

2.11.28.1 Cipher-Algorithms

The cipher algorithms are used for encrypting and decrypting data. Select one or more of the available algorithms.

Console path:

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

Possible values:

3des-cbc
3des-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
blowfish-ctr
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
chacha20-poly1305
aes128-gcm
aes256-gcm

Default:

3des-cbc

3des-ctr

arcfour

arcfour128

arcfour256

blowfish-cbc

blowfish-ctr

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

2.11.28.2 MAC algorithms

The Message Authentication Code (MAC) algorithms are used to check the integrity of messages. Select one or more from the available Encrypt-and-MAC or Encrypt-then-MAC algorithms.

For SSH algorithms, client preference always applies. The client sets the algorithm and usually picks the first match from its list of available algorithms. If necessary, adjust the list of your clients.

Console path:

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

Possible values:

hmac-md5-96
hmac-md5
hmac-sha1-96
hmac-sha1
hmac-sha2-256-96
hmac-sha2-256
hmac-sha2-512-96
hmac-sha2-512
hmac-md5-96-etm
hmac-md5-etm
hmac-sha1-96-etm
hmac-sha1-etm
hmac-sha2-256-96-etm
hmac-sha2-256-etm
hmac-sha2-512-96-etm
hmac-sha2-512-etm
hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

Default:

hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

2.11.28.3 Key-Exchange-Algorithms

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

Console path:

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

Possible values:

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

Default:

diffie-hellman-group-exchange-sha256

ecdh-sha2

curve25519-sha256

curve448-sha512

sntrup761x25519-sha512

diffie-hellman-group14-sha256

diffie-hellman-group16-sha512

2.11.28.7 DH-Groups

The Diffie-Hellman groups are used for the key exchange. Select one or more of the available groups.

Console path:

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

Possible values:

Group-1
Group-5
Group-14
Group-15
Group-16
Group-1; Group-5; Group-14

Default:

Group-1; Group-5; Group-14

2.11.28.8 Compression

With this setting, you enable or disable compression of data packets for connections using SSH.

Console path:

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

Possible values:

Yes
No

Default:

Yes

2.11.28.9 Elliptic curves

This is where you select the (NIST) curves used by the device for the elliptic curve cryptography (ECC).

All of the NIST curves given here are suitable for the ECDH key agreement, whereas host keys are based on the curves `nistp256` and `nistp384`.

Console path:

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

Possible values:

nistp256
nistp384
nistp521

Default:

nistp256

nistp384

nistp521

2.11.28.10 SFTP server

This menu allows you to adjust the settings for the SFTP server.

Console path:

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

2.11.28.10.1 Operating

You enable or disable the SFTP server with this setting.

Console path:

Setup > **Config** > **SSH** > **SFTP-Server**

Possible values:

Yes
No

Default:

Yes

2.11.28.11 Keepalive interval

Using this parameter, you configure the SSH keepalives for server-side connections. The parameter defines the interval in which the internal LCOS SSH server sends keepalives to keep a connection open.

Console path:

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

Possible values:

0 … 99999 Seconds

Special values:

0

This value disables the function.

Default:

60

2.11.28.12 Operating

Activate or deactivate the use of SSH here.

Console path:

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

2.11.28.13 Port

Specify the SSH port.

Console path:

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

Possible values:

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

Default:

22

2.11.28.14 Authentication methods

This menu contains the authentication methods for all interfaces

Console path:

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

2.11.28.14.1 Ifc.

Shows the selected interface (e.g. "LAN").

Console path:

Setup > **Config** > **SSH** > **Authentication-Methods**

2.11.28.14.2 Methods

This entry is used to set the authentication method used for the selected interface (e.g. "LAN").

Console path:

Setup > **Config** > **SSH** > **Authentication-Methods**

Possible values:

All
All available methods are supported for the authentication.

Keyboard-Interactive
User input is required for authentication.

Password
A password is required for authentication.

Password+Keyboard-Interactive
A password and user input are required for authentication.

Password+Public-Key
A password in combination with a public SSH key are used for authentication.

Password+Keyboard-Interactive+Public-Key
A password in combination with user input and a public SSH key are used for authentication.

Default:

All

2.11.28.15 Signing-Hostkey-Algorithms

The host key algorithms are used to authenticate hosts. Select one or more of the available algorithms.

Console path:

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

Possible values:

ssh-rsa
ssh-dss
ecdsa-sha2
ssh-ed25519
rsa-sha2-256
rsa-sha2-512
ssh-ed448

Default:

ssh-rsa

ssh-dss

2.11.28.16 Verifyable-Hostkey-Algorithms

The host key algorithms are used to authenticate hosts. Select one or more of the available algorithms.

Console path:

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

Possible values:

ssh-rsa
ssh-dss
ecdsa-sha2
ssh-ed25519
rsa-sha2-256
rsa-sha2-512
ssh-ed448

Default:

ssh-rsa

ssh-dss

2.11.28.17 Min-RSA-Hostkey-Length

This parameter defines the minimum length of your RSA hostkeys.

Console path:

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

Possible values:

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

Default:

2048

2.11.28.18 Max-RSA-Hostkey-Length

This parameter defines the maximum length of your RSA host keys.

Console path:

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

Possible values:

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

Default:

8192

2.11.28.19 Nonauth-Disconnect-Time

This parameter defines the time in seconds after which the SSH connection is terminated, if the client has not yet authenticated itself.

Console path:

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

Possible values:

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

Default:

120

2.11.28.20 Max-Auth-Tries

Defines the number of consecutive attempts allowed for public key authentication. When the configured value is reached, the SSH server terminates the connection.

Console path:

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

Possible values:

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

Default:

6

Special values:

0

Function disabled.

2.11.29 Telnet-SSL

The parameters for Telnet-SSL connections are specified here.

Console path:

Setup > **Config**

2.11.29.2 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

2.11.29.3 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.11.29.4 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.11.29.5 Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.11.29.6 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

On
Off

Default:

On

2.11.29.7 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

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

Allowed
The device permits renegotiations with the remote station.

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

Default:

Allowed

2.11.29.8 Elliptic curves

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

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.11.29.10 PORT

This port is used for encrypted configuration connections via telnet.

Console path:
Setup > **Config** > **Telnet-SSL**

Possible values:
0 … 65535

Default:
992

2.11.29.11 Operating

Enables or disables Telnet SSL.

Console path:
Setup > **Config** > **Telnet-SSL**

Possible values:

Yes
Telnet SSL is used.

No
Telnet SSL is disabled.

Default:

Yes

2.11.29.22 Signature hash algorithms

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

Console path:

Setup > **Config** > **Telnet-SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

2.11.31 Anti-theft protection

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations do not stop third parties from operating RAS access, LAN connectivity or VPN connections that are set up in the device: A thief could gain access to a protected network. The device's operation can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

GPS location verification

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically activates the GPS module and checks if it is located at the "correct" position. The router module only switches on if the check is positive. After location verification has been carried out the GPS module is switched off again, unless it was activated manually.

Console path:

Setup > **Config**

2.11.31.1 Enabled

Activate GPS location verification with this option.

Console path:

Setup > **Config** > **Anti-Theft-Protection**

Possible values:

No
Yes

Default:

No

2.11.31.8 Deviation[m]

Deviation from the intended position in meters.

Console path:

Setup > **Config** > **Anti-Theft-Protection**

Possible values:

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

Default:

empty

2.11.31.9 Longitude[deg]

Longitude of the location where the device is to operate.

Console path:

Setup > **Config** > **Anti-Theft-Protection**

Possible values:

Max. 12 characters from `[0-9]+-.`

Default:

empty

2.11.31.10 Latitude[deg]

Latitude of the location where the device is to operate.

Console path:

Setup > **Config** > **Anti-Theft-Protection**

Possible values:

Max. 11 characters from `[0-9]+-.`

Default:

empty

2.11.31.12 Get-GPS-position

This option allows the device to determine the geographical coordinates of its current location. Once the configuration is written back to the device, the current longitude and latitude are entered automatically, assuming that location verification is activated and a valid GPS position is available. Subsequently this option is automatically deactivated again.

Console path:

Setup > **Config** > **Anti-Theft-Protection**

Possible values:

Yes
No

Default:

No

2.11.32 Reset button

The reset button offers two basic functions—boot (restart) and reset (to the factory settings)—which are called by pressing the button for different lengths of time.

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button is controlled with this setting.

After a reset, the access point returns to "managed mode", in which case the configuration cannot be directly accessed via the WLAN interface!

After resetting, the device starts completely unconfigured and all settings are lost. If possible be sure to backup the current device configuration before resetting.

The settings "Ignore" or "Boot only" makes it impossible to reset the configuration to the factory settings or to load the rollout configuration with a reset. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device—this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available in the LCOS reference manual.

Console path:

Setup > **Config**

Possible values:

Ignore

The button is ignored.

Boot only

With a suitable setting, the behavior of the reset button can be controlled; the button is then ignored or a press of the button prompts a restart only, however long it is held down.

Reset or boot

With this setting, the reset button fulfills different functions depending upon how long the key remains pressed:

Less than 5 seconds: Boot (restart), whereby the user-defined configuration is loaded from the configuration memory. If the user-defined configuration is empty, then the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. Similarly, the factory settings are loaded if the first memory space is empty.

Longer than 5 seconds until the first time that all device LEDs light up: Configuration reset (deletes the configuration memory) followed by a restart. In this case the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible

when all LEDs on the device light up briefly in red. The factory settings are loaded if the first memory space is empty.

Longer than 15 seconds until the second time that all device LEDs light up: Activating the rollout configuration and deleting the user-defined configuration After restarting, the rollout configuration is started from memory space 2. The loading of the rollout configuration is visible when all LEDs on the device light up twice briefly in red. The factory settings are loaded if the second memory space is empty.

Further information about the different boot configurations are to be found in the reference manual.

Ignore

The button is ignored.

Default:

Reset or boot

2.11.33 Outband aging minutes

Specify here the number of minutes after which an inactive serial connection (e.g. via Hyper Terminal) is automatically terminated.

Console path:

Setup > **Config**

Possible values:

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

Default:

1

2.11.34 Telnet-Operating

This entry is used to enable or disable Telnet.

Console path:

Setup > **Config**

Possible values:

Yes

Telnet is enabled.

No

Telnet is disabled.

Default:

Yes

2.11.36 TFTP-Operating

The trivial file transfer protocol (TFTP) is a simpler variant of the file transfer protocol (FTP). In contrast to FTP, TFTP permits the reading or writing of files via UDP only.

This entry is used to enable or disable the TFTP.

Console path:

Setup > **Config**

Possible values:

No
Yes
Sysinfo-only

The port is kept open and the device responds to a sysinfo request. As a result it is displayed in LANconfig and, in particular, it will be found when searching for devices. However, no configuration can be uploaded to the device. Since this protocol transmits unencrypted, sensitive data could be intercepted on the network.

Default:

Sysinfo-only

2.11.39 License expiry email

The license to use a product can be restricted to a set validity period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires by an e-mail to the address configured here.

Console path:

Setup > **Config**

2.11.40 Crash message

Here you specify the message that appears in the bootlog when the device crashes.

Console path:

Setup > **Config**

Possible values:

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

Default:

LCOS-Watchdog

2.11.41 Admin gender

Enter the gender of the Admin.

Console path:

Setup > **Config**

Possible values:

Unknown
Male
Female

Default:

Unknown

2.11.42 Assert action

This parameter affects the behavior of the device when it checks the firmware code.

The settings for this parameter are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **Config**

Possible values:

log_only
reboot

Default:

log_only

2.11.43 Function keys

The function keys enable the user to save frequently used command sequences and to call them easily from the command line. In the appropriate table, commands are assigned to function keys F1 to F12 as they are entered in the command line.

Console path:

Setup > **Config**

2.11.43.1 Key

Name of function key.

Console path:

Setup > **Config** > **Function-keys**

Possible values:

F1

Function keys F1 to F12.

F2 – F12

Default:

F1

2.11.43.2 Figure

Description of the command/shortcut to be run on calling the function key in the command line.

Console path:

Setup > **Config** > **Function-keys**

Possible values:

All commands/shortcuts possible in the command line.

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

Default:

empty

Special values:

"^"

The caret symbol (^) is used to represent special control commands with ASCII values below 32.

Command	Meaning
^A	Ctrl-A (ASCII 1)
^Z	Ctrl-Z (ASCII 26)
^[	Escape (ASCII 27)
^M	Mention return/enter. This character is useful if you enter a command with the function key and wish to send it immediately.
^^	A double caret symbol stands for the caret symbol itself.

If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. By entering caret + A the Windows operating system outputs an **Â**. To enter the caret character itself, enter a space in front of the subsequent characters. Sequence **^A** is then formed from caret symbol + space + A.

2.11.45 Configuration date

This parameter allows LANconfig to be used to set the date of a configuration.

This value exists only in the SNMP chain.

Console path:

Setup > **Config** > **Config-Date**

Possible values:

Valid configuration date

2.11.50 LL2M

The menu contains the settings for LANCOM layer-2 management.

Console path:

Setup > **Config**

2.11.50.1 Operating

Enables/disables the LL2M server. An LL2M client can contact an enabled LL2M server for the duration of the time limit following device boot/power-on.

Console path:

Setup > **Config** > **LL2M**

Possible values:

Yes
No

Default:

Yes

2.11.50.2 Time limit

Defines the period in seconds during which an enabled LL2M server can be contacted by an LL2M client after device boot/power-on. The LL2M server is disabled automatically after expiry of the time limit.

Console path:

Setup > **Config** > **LL2M**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

This value disables the time limit. In this state the LL2MServer remains permanently active.

2.11.50.3 Crypto-Algorithms

This item is used to limit the range of encryption algorithms used for LL2M connections. This setting applies to the server and client mode. The Simple algorithm uses the cleartext password as the basis for key derivation, while the other two algorithms use an encrypted password as the basis, which is encrypted with either SHA-256 or SHA-512. Simple must remain enabled for communicating with LCOS versions before LCOS 10.40.

Note that the algorithm selection must be consistent with the selected password encryption algorithm: For example, if SHA-512 is used to encrypt admin passwords (see *2.11.89.2 Crypto-Algorithm* on page 384) and cleartext passwords are not stored (see *2.11.89.1 Keep-Cleartext* on page 384), SHA-512 must not be deactivated here, otherwise the device cannot be reached via LL2M.

Console path:

Setup > **Config** > **LL2M**

Possible values:

Simple
SHA-256
SHA-512

Default:

Simple

SHA-256

SHA-512

2.11.51 Sync

In this directory, you configure the automatic configuration synchronization.

Console path:

Setup > **Config**

2.11.51.1 Operating

Activates or deactivates the automatic configuration synchronization.

Console path:

Setup > **Config** > **Sync**

Possible values:

No
Yes

Default:

No

2.11.51.2 New cluster

Here you can configure the scope of a configuration synchronization.

Console path:

Setup > **Config** > **Sync**

2.11.51.2.1 Name

Enter an identifier for this entry.

Console path:

Setup > **Config** > **Sync** > **New Cluster**

Possible values:

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

Default:

Default

2.11.51.2.2 Cluster members

This table lists devices that participate in the automatic configuration synchronization.

Console path:

Setup > **Config** > **Sync** > **New Cluster**

2.11.51.2.2.1 Idx.

Index for this entry in the list.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Group Members**

Possible values:

Max. 5 characters from `0123456789`

Default:

empty

2.11.51.2.2.2 Address

IP address of the corresponding device.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Group Members**

Possible values:

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

Possible arguments:

IPv4 address
IPv6 address

Default:

empty

2.11.51.2.3 Menu nodes

Here you configure which configuration items are to be contained in the automatic configuration synchronization. This enables you to include or exclude values, tables, and entire menus.

Console path:

Setup > **Config** > **Sync** > **New Cluster**

2.11.51.2.3.1 Idx.

Index for this entry in the list.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Menu Nodes**

Possible values:

Max. 5 characters from `0123456789`

Default:

empty

2.11.51.2.3.2 Include

Specify here whether the specified menu node is included in or excluded from the automatic configuration synchronization.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Menu Nodes**

Possible values:

Include
Exclude

Default:

Include

2.11.51.2.3.3 Path

Enter the path to the menu node. This can be a value, a table, or a complete menu.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Menu Nodes**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

/Setup

2.11.51.2.3.4 SNMP OID

Show the SNMP-ID of the specified menu node.

The display is updated after you save the entry.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Menu Nodes**

Possible values:

2

Default:

2

2.11.51.2.4 Ignored rows

If you include a table into the automatic configuration synchronization, this item is used to determine which rows of this table are to be excluded from it.

Console path:

Setup > **Config** > **Sync** > **New Cluster**

2.11.51.2.4.1 Idx.

Index for this entry in the list.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Ignored Rows**

Possible values:

Max. 5 characters from `0123456789`

Default:

empty

2.11.51.2.4.2 Row index

Here you specify the row number (index) to be excluded from the automatic configuration synchronization.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Ignored Rows**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.11.51.2.4.3 Path

Specify the path to the node of the table that is contained in the automatic configuration synchronization.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Ignored Rows**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

/Setup

2.11.51.2.4.4 SNMP OID

Show the SNMP-ID of the specified table node.

The display is updated after you save the entry.

Console path:

Setup > **Config** > **Sync** > **New Cluster** > **Ignored Rows**

Possible values:

2

Default:

2

2.11.51.2.5 Home

Starts the automatic configuration synchronization for this entry.

Console path:

Setup > **Config** > **Sync** > **New Cluster**

2.11.51.3 TLS connections

In this directory, you specify the address and port to be used by the device to accept incoming configuration changes.

Console path:

Setup > **Config** > **Sync**

2.11.51.3.1 Port

Specify the port to be used by the device to receive incoming configuration changes.

Console path:

Setup > **Config** > **Sync** > **TLS-Connections**

Possible values:

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

0 … 65535

Default:

1941

2.11.51.3.2 Loopback address

Specify the loopback address to be used by the device to receive incoming configuration changes.

Console path:

Setup > **Config** > **Sync** > **TLS-Connections**

Possible values:

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

Possible arguments:

Name of the IP networks whose address should be used
“INT” for the address of the first Intranet
“DMZ” for the address of the first DMZ
LBO…LBF for the 16 loopback addresses
Any valid IPv4 or IPv6 address

Default:

empty

2.11.51.4 Renew snapshot

In this directory you configure the snapshots.

Console path:

Setup > **Config** > **Sync** > **Renew-Snapshot**

2.11.51.4.1 Modification limit

Enter the modification limit here.

Console path:

Setup > **Config** > **Sync** > **Renew-Snapshot**

Possible values:

Max. 10 characters from `0123456789`

Special values:

0

This value disables the function.

Default:

2048

2.11.51.4.2 Kept modifications

This value specifies the number of kept modifications.

Console path:

Setup > **Config** > **Sync** > **Renew-Snapshot**

Possible values:

Max. 10 characters from `0123456789`

0 … 4294967295 Powers of two

Special values:

0

This value disables the function.

Default:

256

2.11.51.4.3 Renew snapshot

This action renews the snapshot.

Console path:

Setup > **Config** > **Sync** > **Renew-Snapshot**

2.11.51.5 Local configuration

In this directory you specify the number of applied and detected modifications.

Console path:

Setup > **Config** > **Sync** > **Local Config**

2.11.51.5.1 Detected modifications

Specify the number of detected modifications.

Console path:

Setup > **Config** > **Sync** > **Local Config**

Possible values:

Max. 10 characters from `0123456789`

2.11.51.5.2 Applied modifications

Specify the number of applied modifications.

Console path:

Setup > **Config** > **Sync** > **Local Config**

Possible values:

Max. 10 characters from `0123456789`

2.11.55 SSL-for-Cron-Table

This menu contains the settings of the Secure Sockets Layer for the links in the cron table.

Console path:

Setup > **Config**

2.11.55.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.11.55.2 Key-exchange algorithms

Here you choose between three different key exchange techniques. You can select multiple techniques. All three are selected by default.

Devices that communicate via an SSL-secured connection regularly exchange encryption keys.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.11.55.3 Crypto-Algorithms

Here you choose between different cryptographic algorithms. You can select multiple algorithms.

The crypto algorithm is a complex translation rule that converts the transmitted information piece by piece into data packets that are of no value to eavesdroppers. The verified recipient reconstructs the original message using a cryptic key.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.11.55.4 Hash algorithms

Here you choose between different hash algorithms. You can select multiple algorithms. All of them are selected by default.

The sent message packets contain checksums for the detection of transmission errors and manipulations. These checksums formed with what are known as hash algorithms. Cryptological hash algorithms are considered to be highly reliable.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

MD5
SHA1
SHA-256
SHA-384
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA-256

SHA-384

SHA2-256

SHA2-384

2.11.55.5 Prefer PFS

The keys used for encoding are constantly changed. If you prefer PFS, an attacker who knows a key can only decode the part of the message encoded with that key. It is impossible to deduce the other keys that were used.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

Yes

Default:

Yes

2.11.55.6 Renegotiations

Specify whether renegotiations are allowed, prohibited, or ignored.

SSL has a security loophole in the form of what is called a renegotiation attack. If you fear an attack of this type, you prohibit renegotiation in general. This then also prevents legal renegotiations!

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

Allowed
Forbidden
Ignored

Default:

Allowed

2.11.55.7 Elliptic curves

Here you choose between three different elliptic curves. You can select multiple curves. All three are selected by default.

Crypto-algorithms are usually executed within mathematical bodies. A mathematical body can be implemented with prime number modules and by means of a discrete elliptic curve.

The mathematical operations on elliptic curves are more complex to compute than operations in finite bodies of a comparable size. The shorter keys, however, allow crypto-systems based on elliptic curves to be faster than crypto-systems of comparable security levels based on a prime number module.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

2.11.55.21 Signature hash algorithms

Here you choose from various signature hash algorithms. You can select multiple algorithms.

Digital signatures are provided with a checksum for the purpose of detecting erroneous transmission or targeted manipulation. This checksum is formed by what are known as hash algorithms. Cryptological hash algorithms are considered to be highly reliable.

Console path:

Setup > **Config** > **SSL-for-Cron-Table**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.11.60 CPU load interval

You can select the time interval for averaging the CPU load. The CPU load displayed in LANmonitor, in the status area, in the display (if fitted), or by SNMP tools is a value which is averaged over the time interval set here. The status area under WEBconfig or CLI additionally display the CPU load values for all four of the optional averaging periods.

Console path:

Setup > **Config**

Possible values:

T1s (arithmetic mean)
T5s (arithmetic mean)
T60s (moving average)
T300s (moving average)

Default:

T60s (moving average)

2.11.65 Error aging minutes

Here you set the length of time in minutes after which the device deletes VPN errors from the status table.

To document sporadic errors, disable this option with the entry `0`.

Console path:

Setup > **Config**

Possible values:

Max. 4 characters from `0123456789`

Default:

0

Special values:

0

Disables this option. Errors will remain in the status table.

2.11.71 Save bootlog

This parameter enables or disables the boot-persistent storage of SYSLOG messages to the flash memory of the device. Bootlog information is not lost even when restarting after a loss of mains power. The bootlog contains information about the boot processes of the device.

If necessary, delte the persistent bootlog memory by entering the command `deletebootlog` anywhere on the command line.

Console path:

Setup > **Config**

Possible values:

Yes
No

Default:

Yes

2.11.72 Save eventlog

This parameter enables or disables the boot-persistent storage of event log messages to the flash memory of the device. Event log information is retained even when restarting after a loss of mains power. The event log contains the information from the table **Status** > **Config** > **Event-Log**. This table stores information on administrator logins and logouts, and on upload and download operations of configurations and firmware files.

If necessary, delte the persistent event log memory by entering the command `deleteeventlog` anywhere on the command line.

Console path:

Setup > **Config**

Possible values:

Yes
No

Default:

Yes

2.11.73 Sort-menu

Using this parameter, you specify whether the device displays menu items in ascending alphabetical order on the console by default. The setting corresponds to the option switch `-s` when listing menu or table contents.

Console path:

Setup > **Config**

Possible values:

No
Yes

Default:

No

2.11.80 Authentication

Various options are available to authenticate with the device and access the management interface.

Since the RADIUS protocol does not allow for a change of passwords, the users logged in via RADIUS cannot change their password in the device.

To manage the necessary data for the RADIUS server, go to **Setup** > **Config** > **Radius** > **Server**. To manage the necessary data for the TACACS+ server, go to **Setup** > **Tacacs+** > **Server**.

Console path:

Setup > **Config**

Possible values:

Internal
The device manages the users internally in the table **Setup** > **Config** > **Admins**.

Radius
A RADIUS server handles the management of the users.

TACACS+
A TACACS+ server handles the management of the users.

Default:

Internal

2.11.81 Radius

If the user has to login to the management interface by authenticating via a RADIUS server, you enter the related server data and the user/administration data here.

Console path:

Setup > **Config**

2.11.81.1 Server

This table contains the settings for the RADIUS server.

Console path:

Setup > **Config** > **Radius**

2.11.81.1.1 Name

Enter a name for the RADIUS server.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

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

Default:

empty

2.11.81.1.2 Server

Enter the IPv4 address of the RADIUS server here.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

Max. 64 characters from `[0-9].`

Default:

empty

2.11.81.1.3 Port

Specify here the port used by the RADIUS server to communicate with the device.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

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

Default:

1812

2.11.81.1.4 Protocol

Specify here the protocol used by the RADIUS server to communicate with the device.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.11.81.1.5 Loopback address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

Name of the IP networks whose addresses are to be used by the device.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If the list of IP networks or loopback addresses contains an entry named "DMZ", then the associated IP address will be used.

LB0 – LBF for one of the 16 loopback addresses
Any valid IP address.
empty

Default:

2.11.81.1.6 Secret

Enter the password for accessing the RADIUS server and repeat it in the second input field.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

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

Default:

empty

2.11.81.1.7 Backup

Specify the name of the alternative RADIUS server to which the device forwards requests when the first RADIUS server cannot be reached.

The backup server requires an additional entry in the Server table.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

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

Default:

empty

2.11.81.1.8 Category

Set the category for which the RADIUS server applies.

You can select No, one or both categories.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

Authentication
Accounting

Default:

Authentication

2.11.81.1.9 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **Config** > **Radius** > **Server**

Possible values:

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

Default:

empty

2.11.81.1.10 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **Config** > **RADIUS** > **Server**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.11.81.2 Access rights transfer

The RADIUS server stores the user authorization. When a request arrives, the RADIUS server returns the access rights, privileges and the login data to the device, which then logs in the user with the appropriate rights.

Normally access rights are set in the RADIUS management privilege level (attribute 136), so that the device only needs to map the returned value to its internal access rights (option **mapped**). The attribute can have the following values, which are mapped by the device:

Attribute	Access rights
1	User, read-only
3	User, write-only
5	Admin, read-only, no trace rights
7	Admin, read and write, no trace rights
9	Admin, read-only
11	Admin, read and write
15	Supervisor

The device maps all other values to 'no access'.

However, it may be that the RADIUS server additionally needs to transfer privileges, or that attribute 136 is already used for other purposes and/or for vendor-specific authorization attributes. If this is the case, you should select Vendor-Specific attributes. These attributes are specified as follows, based on the vendor ID '2356':

- Privileges ID: 11

› Function rights ID: 12

The values transferred for access rights are identical to those mentioned above. If the RADIUS server should also transfer privileges, you achieve this as follows:

1. Open the device console.
2. Change to the directory **Setup** > **Config** > **Admins**.
3. The command `set ?` shows you the current mapping of privileges to the corresponding hexadecimal code (e.g. `Device-Search (0x80)`).
4. In order to combine privileges, you add their hex values.
5. You can use this decimal value as the Privileges ID to transfer the corresponding privileges.
6. You can use this decimal value as the Privileges ID to transfer the corresponding privileges.

Console path:

Setup > **Config** > **Radius**

Possible values:

Vendor specific
Mapped
Shell privilege

Default:

Vendor specific

2.11.81.3 Accounting

Here you specify whether the device should record the user's session. In this case it stores the session data including the start time, end time, user name, authentication mode and, if available, the port used.

Console path:

Setup > **Config** > **Radius**

Possible values:

No
Yes

Default:

No

2.11.89 Passwords

This item contains settings for the algorithm used to create the password hash.

Console path:

Setup > **Config**

2.11.89.1 Keep-Cleartext

As of LCOS 10.40 an algorithm is used to store the main device password and the administrator passwords in encrypted form as a hash value. Specify here whether the cleartext password is also retained.

Console path:

Setup > **Config** > **Passwords**

Possible values:

Yes

The main device password and the administrator passwords are internally also stored in cleartext. This means that the password can still be displayed in LANconfig, and that access points with an LCOS version earlier than 10.40 can still be managed by a WLC or the WLC option. The password is not visible from the CLI.

If you wish to retain the option of downgrading the firmware to an LCOS version earlier than 10.40, this option must be set.

If a firmware downgrade is made to an LCOS version prior to 10.40 that does not support encrypted passwords, the password will be deleted. Access to the router from the LAN or WLAN is then possible without a password! Access from the WAN is not possible without a password!

No

The main device password and the administrator passwords are internally stored in hashed form only.

Default:

No

2.11.89.2 Crypto-Algorithm

The algorithm used to encrypt the passwords.

Console path:

Setup > **Config** > **Passwords**

Possible values:

SHA-256
SHA-512

Default:

SHA-512

2.11.89.3 Rounds

This value determines how often the encryption algorithm is used. The more rounds are calculated, the higher the resistance to brute-force attacks. This does slow down the actual work with passwords. The 5000 rounds specified in the configuration offer a high level of security with a good working speed.

Console path:

Setup > **Config** > **Passwords**

Possible values:

1000 … 999999999

Default:

5000

2.11.89.4 Password-Complexity

Use this menu to configure password-length and complexity requirements.

Console path:

Setup > **Config** > **Passwords**

2.11.89.4.1 Minimum-Length

Configure the minimum number of characters for passwords here.

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

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

Default:

8

2.11.89.4.2 Unique-Characters

Configure the required number of unique characters for passwords here.

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

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

Default:

3

2.11.89.4.3 Complexity-Classes

Configure the required number of complexity classes for passwords here. Complexity classes are lower and upper case letters, numbers, and special characters. If the setting is 2, the password would have to contain characters from at least two of these complexity classes.

Console path:

Setup > **Config** > **Passwords** > **Password-Complexity**

Possible values:

0 … 4

Default:

3

2.11.90 LED mode

You set the operating mode of the device LEDs here.

The "LED-Test" function is available despite the LEDs being disabled.

Console path:

Setup > **Config**

Possible values:

On

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

Default:

On

2.11.91 LED off seconds

You specify the delay in seconds after which the LEDs are disabled following a restart.

If you change this value and save it within the previously set time, you should restart the timer.

Console path:

Setup > **Config**

Possible values:

Max. 4 characters `0123456789`

Default:

300

2.11.92 Rollout agent

This menu allows you to configure the settings for the rollout agent.

Console path:

Setup > **Config**

2.11.92.1 Operating

This entry determines how the rollout agent operates.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

No

The rollout agent is disabled.

Yes

The rollout agent is enabled and transmits the rollout data that is configured in the device to the rollout server.

DHCP initiated

The rollout agent is enabled. It processes the information received from the DHCP server in the DHCP option 43.

The "DHCP-initiated" operating mode does not overwrite manually configured attributes. This makes it possible to perform a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

Default:

DHCP initiated

2.11.92.2 Configuration server

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.3 Firmware server

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.4 User name

Set the user name used by the rollout agent to log on to the rollout server.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.5 Password

Set the user password used by the rollout agent to log on to the rollout server.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.6 Project number

This entry specifies the rollout project number for the rollout agent.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.7 Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.8 Reboot time

Here you set the time after which the device reboots after a rollout.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

0

2.11.92.9 Request-Interval

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

0

Special values:

0

The next attempt starts in 1 minute.

2.11.92.10 TAN

Use this entry to specify the rollout TAN.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.11 Device number

Contains the device number of the device that is running the rollout agent.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

empty

2.11.92.12 Request delay

This entry contains the delay time in seconds for a rollout request.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

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

Default:

0

2.11.92.13 Request time random

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

No
Yes

Default:

No

2.11.92.14 Omit certificate check

Specifies whether a server certificate verification is carried out on HTTPS connections.

Console path:

Setup > **Config** > **Rollout-Agent**

Possible values:

No
A certificate check is carried out.
Yes
No certificate check is carried out.

Default:

No

2.11.92.15 SSL

This menu contains the SSL configuration for the Rollout Agent.

Console path:

Setup > **Config** > **Rollout-Agent**

2.11.92.15.1 Versions

This entry specifies the protocol versions allowed for the Rollout Agent.

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.11.92.15.2 Key-exchange algorithms

This is where you specify the algorithms for the key exchange.

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.11.92.15.3 Crypto-Algorithms

This entry specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.11.92.15.4 Hash algorithms

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

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

MD5
SHA1
SHA-256
SHA-384
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA-256

SHA-384

SHA2-256

SHA2-384

2.11.92.15.5 Prefer PFS

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.11.92.15.6 Renegotiations

Here you select whether new negotiations are allowed.

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

Forbidden
Allowed
Ignored

Default:

Allowed

2.11.92.15.7 Elliptic curves

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

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

2.11.92.15.21 Signature hash algorithms

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

Console path:

Setup > **Config** > **Rollout-Agent** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA-224-RSA
SHA-256-RSA
SHA-384-RSA
SHA-512-RSA

Default:

MD5-RSA

SHA1-RSA

SHA-224-RSA

SHA-256-RSA

SHA-384-RSA

SHA-512-RSA

2.11.92.16 Use OCSP

Here you configure the menu **Use OCSP**.

Console path:

Setup > **Config** > **Rollout-Agent**

2.11.93 Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for the main device password and the passwords of other administrators:

- The length of the password must be at least 8 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

Console path:

Setup > **Config**

Possible values:

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

Yes

2.11.94 DSCP marking

Internal LCOS applications can be marked with configurable DiffServ CodePoints (DSCP). This allows downstream hardware to recognize and prioritize these packets. Further information about DiffServ CodePoints is available in the Reference Manual under the section Quality of Service.

This configuration marks only the control messages of the respective protocols.

Console path:

Setup > **Config**

2.11.94.1 Application

Column with the internal applications.

Console path:

Setup > **Config** > **DSCP-Marking**

2.11.94.2 DSCP

Column with the DiffServ codepoints. Default values are listed for the possible internal applications.

Console path:

Setup > **Config** > **DSCP-Marking**

Possible values:

BGP

CS6

OSPF

CS6

RIP

CS6

IKE

CS6

Incl. Dynamic VPN UDP packets, but not supported with SSL encapsulation.

TACACS

BE/CS0

SNMP

BE/CS0

L2TP

CS6

PPTP

CS6

LISP

CS6

TFTP

BE/CS0

ICMP

BE/CS0

2.11.97 Configuration-Upload-Check

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

Console path:

Setup > **Config**

Possible values:

tolerant

Unknown OIDs are accepted.

strict

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

Default:

tolerant

2.12 WLAN

This menu contains the settings for wireless LAN networks.

Console path:

Setup

2.12.3 Heap reserve

The heap reserve specifies how many blocks in the LAN heap can be reserved for direct communication (Telnet) with the device. If the number of blocks in the heap falls below the specified value, received packets are dropped immediately (except for TCP packets sent directly to the device).

Console path:

Setup > **WLAN**

Possible values:

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

Default:

10

2.12.8 Access mode

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

Console path:

Setup > **WLAN**

Possible values:

Filter out data from listed stations, transfer all other.
Transfer data from the listed stations, authenticate all others via RADIUS or filter them out.

Default:

Filter out data from listed stations, transfer all other.

2.12.12 IAPP protocol

Access points use the Access Point Protocol (IAPP) to exchange information about their associated clients. This information is used in particular when clients roam between different access points. The new access point informs the former one of the handover, so that the former access point can delete the client from its station table.

Console path:

Setup > **WLAN**

Possible values:

Yes
No

Default:

Yes

2.12.13 IAPP-Announce-Interval

This is the interval (in seconds) with which the access points broadcast their SSIDs.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

120

2.12.14 IAPP-Handover-Timeout

If the handover is successful, the new access point informs the former access point that a certain client is now associated with another access point. This information enables the former access point to delete the client from its station table. This stops packets being (unnecessarily) forwarded to the client. For this time space (in milliseconds) the new access point waits before contacting the former access point again. After trying five times the new access point stops these attempts.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

1000

2.12.26 Inter-SSID-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. Communications between clients in different SSIDs can be allowed or stopped with this option. For models with multiple WLAN modules, this setting applies globally to all WLANs and all modules.

Communications between clients in a logical WLAN is controlled separately by the logical WLAN settings (Inter-Station-Traffic). If the Inter-SSID-Traffic is activated and the Inter-Station-Traffic deactivated, a client in one logical WLAN can communicate with clients in another logical WLAN. This option can be prevented with the VLAN settings or protocol filter.

Console path:

Setup > **WLAN**

Possible values:

Yes
No

Default:

Yes

2.12.27 Supervise stations

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the access point regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

Console path:

Setup > **WLAN**

Possible values:

On
Off

Default:

Off

2.12.29 RADIUS access check

This menu contains the settings for the RADIUS access checking.

Console path:

Setup > **WLAN**

Possible values:

On
Off

Default:

Off

2.12.29.2 Auth.-Port

Port for communication with the RADIUS server during authentication

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

0 … 65535

Default:

1812

2.12.29.3 Secret

Password used to access the RADIUS server

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.5 Backup auth. port

Port for communication with the backup RADIUS server during authentication.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

0 … 65535

Default:

1812

2.12.29.6 Backup secret

Password used to access the backup RADIUS server.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.7 Response lifetime

This value defines the lifetime for an entry stored on the device for a MAC check that was rejected by the RADIUS server.

If a RADIUS server is used to check the MAC addresses of wireless clients, the device forwards all requests from wireless clients to the RADIUS server. If a MAC address is listed in the RADIUS server as blocked, then the reject response from the RADIUS server is stored in the device for the time set here. If the device receives repeated requests from blocked MAC addresses, the requests are not forwarded to the RADIUS server.

Recently cached MAC address entries can be viewed in the table **1.3.48 RADIUS-Cache**.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

0 … 4294967295

Default:

15

2.12.29.8 Password source

Here you specify whether the device uses the shared secret or the MAC address as the password during authentication at the RADIUS server.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

Secret
MAC address

Default:

Secret

2.12.29.9 Recheck cycle

If you select a value greater than zero, the device checks your MAC address not only at login but also during the connection in the specified cycle in seconds. If you specify zero, the MAC address is only checked at login. Cyclical rechecking enables the device to recognize, for example, a change in bandwidth limits for a MAC address. In this case the client remains logged on and the connection remains intact.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

0 … 4294967295

Default:

0

2.12.29.10 Provide server database

Activate this option if the MAC address list is provided by a RADIUS server.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No
Yes

Default:

Yes

2.12.29.11 Loopback address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If you have configured loopback addresses, you can specify them here as source address.

If there is an interface named "DMZ", then its address is used.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.
empty

Default:

2.12.29.12 Backup-Loopback-Address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If you have configured loopback addresses, you can specify them here as source address.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.
empty

Default:

2.12.29.13 Protocol

Protocol for communication between the backup RADIUS server and the clients.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.12.29.14 Backup-Protocol

Protocol for communication between the backup RADIUS server and the clients.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.12.29.15 Force recheck

Using this action you manually trigger an immediate RADIUS access check. You can enter optional parameters for the command in the input field. The command expects one or more MAC addresses of registered clients as an argument. For these clients, the initial check of their MAC address using the RADIUS server will be repeated. Multiple MAC addresses can be separated with spaces.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

MAC address(es) of registered clients using spaces as separators.
empty

Default:

2.12.29.16 Server host name

Here you enter the IP address (IPv4, IPv6) or hostname of the backup RADIUS server used by the RADIUS client to check the authorization of WLAN clients by means of the MAC address (authentication).

The RADIUS client automatically detects which address type is involved.

To use the RADIUS functionality for WLAN clients, in LANconfig you go to **Wireless LAN** > **Stations** and, for the **Filter stations** parameter, you select the option "Transfer data from the listed stations, authenticate all others via RADIUS or filter them out". You also need to set the general values for retry and timeout in the RADIUS section.

In the RADIUS server, you must enter the WLAN clients as follows:

- The user name is the MAC address in the format AABBCC-DDEEFF.
- The password for all users is identical to the key (shared secret) for the RADIUS server.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.17 Backup server hostname

Here you enter the IP address (IPv4, IPv6) or hostname of the backup RADIUS server used by the RADIUS client to check the authorization of WLAN clients by means of the MAC address (authentication).

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.18 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.19 Backup attribute values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

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

Default:

empty

2.12.29.21 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.12.29.22 Backup-Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.12.36 Country

The device needs to be set with the country where it is operating in order for the WLAN to use the parameters approved for the location.

If you select the value **unknown**, the device allows only those parameters that are approved worldwide!

Console path:

Setup > **WLAN**

Possible values:

Select from the list of countries.
Europe

Default:

Europe

2.12.38 ARP handling

A station in the LAN attempting to establish a connection to a WLAN station which is in power-save mode will often fail or only succeed after a considerable delay. The reason is that the delivery of broadcasts (such as ARP requests) to stations in power-save mode cannot be guaranteed by the base station.

If you activate ARP handling, the base station responds to ARP requests on behalf of the stations associated with it, thus providing greater reliability in these cases.

As of LCOS version 8.00, this switch activates a similar treatment for IPv6 neighbor solicitations.

Console path:

Setup > **WLAN**

Possible values:

On
Off

Default:

On

2.12.41 Mail-Address

Information about events in the WLAN is sent to this e-mail address if this is enabled with the 2.12.141 switch.

An SMTP account must be set up to make use of the e-mail function.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

empty

2.12.44 Allow-Illegal-Association-Without-Authentication

The ability of the device to associate with a WLAN without authentication is enabled or disabled with this parameter.

Console path:

Setup > **WLAN**

Possible values:

Yes
No

Default:

No

2.12.45 RADIUS accounting

The accounting function in the device can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

Console path:

Setup > **WLAN**

Possible values:

Yes
No

Default:

No

2.12.45.8 Interim-Update-Period

The accounting function in the device can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate a restart.

Console path:

Setup > **WLAN** > **RADIUS-Accounting**

Possible values:

0 … 4289999999

Default:

0

2.12.45.9 Excluded VLAN

Here you enter the ID of the VLAN that the device is to exclude from RADIUS accounting. The RADIUS server then receives no information about the traffic in that VLAN.

Console path:

Setup > **WLAN** > **RADIUS-Accounting**

Possible values:

0 … 9999

Default:

0

2.12.45.14 Restart accounting

This feature allows the device to end all running wireless LAN accounting sessions by sending an 'accounting stop' to the RADIUS server. This is helpful, for example, at the end of a billing period.

Console path:

Setup > **WLAN** > **RADIUS-Accounting**

2.12.45.17 Servers

This table provides the option to specify alternative RADIUS accounting servers for logical WLAN interfaces. This means that you can use special accounting servers for selected WLAN interfaces instead of the globally specified server.

Console path:

Setup > **WLAN** > **RADIUS-Accounting**

2.12.45.17.1 Name

Name of the RADIUS server performing the accounting for WLAN clients. The name entered here is used to reference that server from other tables.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

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

Default:

empty

2.12.45.17.3 Port

Port for communication with the RADIUS server during accounting

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

0 … 65535

Default:

0

2.12.45.17.4 Key value

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that specified in the accounting server.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

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

Default:

empty

2.12.45.17.5 Loopback-Addr.

You have the option to enter a different address here (name or IP) to which the RADIUS accounting server sends its reply message. To do this, select from:

- Name of the IP network (ARF network), whose address should be used.
- `INT` for the address of the first Intranet

- `DMZ` for the address of the first DMZ

  If an interface with the name "DMZ" already exists, the device will select that address instead.

- `LB0…LBF` for one of the 16 loopback addresses or its name
- Any IPv4 address

If the source address set here is a loopback address, these will be used on the remote client. **unmasked** !

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

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

Default:

empty

2.12.45.17.6 Protocol

Using this item you specify the protocol that the accounting server uses.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.12.45.17.7 Backup

Enter the name of the RADIUS backup server used for the accounting of WLAN clients if the actual accounting server is not available. This allows you to specify a backup chaining of multiple backup servers.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

Name from **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**

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

Default:

empty

2.12.45.17.8 Host name

Here you enter the IPv4 or IPv6 address or the hostname of the RADIUS server used by the RADIUS client for the accounting of WLAN clients.

The RADIUS client automatically detects which address type is involved.

You also need to set the general values for retry and timeout in the RADIUS section.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

IPv4/IPv6 address or hostname, max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

2.12.45.17.9 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Possible values:

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

Default:

empty

2.12.47 Idle timeout

This is the time in seconds after which a client is disconnected if the access point has not received any packets from it.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

900

2.12.50 Signal averaging

This menu contains the settings for signal averaging.

The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN**

2.12.50.1 Method

Method for signal averaging.

The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Signal-Averaging**

Possible values:

Standard
Filtered

Default:

Standard

2.12.50.2 Standard parameters

This menu contains the configuration of the default parameters for signal averaging.

The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Signal-Averaging**

Possible values:

Standard
Filtered

Default:

Standard

2.12.50.2.1 Factor

Factor for the signal averaging.

The settings for signal averaging are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Signal-Averaging** > **Standard-Parameters**

Possible values:

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

Default:

4

2.12.51 Rate adaption

This menu contains the settings for the rate-adaption algorithm.

Console path:

Setup > **WLAN**

2.12.51.2 Initial rate

The initial rate determines the starting bit rate that the algorithm uses to determine the optimal bit rate.

Console path:

Setup > **WLAN** > **Rate-Adaptation**

Possible values:

Minimum
RSSI-dependent

Default:

Minimum

2.12.51.3 Ministrel averaging factor

The averaging factor used for recalculating the net rates for each bit rate according to the Minstrel method.

Console path:

Setup > **WLAN** > **Rate-Adaptation**

Possible values:

0 … 99

Default:

75

2.12.51.4 Standard averaging factor

The averaging factor used for recalculating the net rates for each bit rate according to the standard method.

Console path:

Setup > **WLAN** > **Rate-Adaptation**

Possible values:

0 … 99

Default:

0

2.12.51.5 Method

Sets the method of rate adaptation.

Console path:

Setup > **WLAN** > **Rate-Adaptation**

Possible values:

Standard
Minstrel

Default:

Minstrel

2.12.60 IAPP-IP-Network

Here you select the ARF network which is to be used as the IAPP-IP network.

Console path:

Setup > **WLAN**

Possible values:

Select from the list of ARF networks defined in the device.
empty

Default:

Possible values:

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

Default:

empty

Special values:

empty

If no IAPP-IP network is defined, IAPP announcements are transmitted on all of the defined ARF networks.

2.12.70 VLAN-Groupkey-Mapping

This table contains the mapping of VLAN group keys to the logical WLAN networks.

Console path:

Setup > **WLAN**

2.12.70.1 Network

Contains the name of a WLAN network registered in the device.

Console path:

Setup > **WLAN** > **VLAN-groupkey-mapping**

2.12.70.2 VLAN-ID

Contains the VLAN ID assigned to the logical WLAN network.

Console path:

Setup > **WLAN** > **VLAN-groupkey-mapping**

Possible values:

1 … 4094

Default:

1

2.12.70.3 Groupkey index

The table contains the group key index.

Console path:

Setup > **WLAN** > **VLAN-groupkey-mapping**

Possible values:

1 … 3

2.12.71 VLAN no interstation traffic

This table contains combinations of SSIDs and VLANs for which data exchange between clients should be prohibited.

Console path:

Setup > **WLAN**

2.12.71.1 Network

From the list of available SSIDs, select the network for which data exchange between clients should be prohibited.

Console path:

Setup > **WLAN** > **VLAN-No-Interstation-Traffic**

2.12.71.2 VLAN-ID

Here you specify the VLAN ID for which data exchange between clients should be prohibited.

Console path:

Setup > **WLAN** > **VLAN-No-Interstation-Traffic**

Possible values:

1 … 4094

Default:

0

2.12.80 Dual roaming

Here is where you manage the roaming behavior of devices with multiple WLAN modules.

Console path:

Setup > **WLAN**

Possible values:

1 … 3

2.12.80.1 Group

Determines whether all WLAN modules participate in dual-roaming.

Console path:

Setup > **WLAN** > **Dual-Roaming**

Possible values:

Off
WLAN-1 + WLAN-2

Default:

Off

2.12.80.2 Block time ms

Using this setting you specify the lockout period for time-staggered roaming of the WLAN modules in dual-radio clients.

If you enable dual roaming, your dual-radio device operates both WLAN modules in client mode. With dual roaming, this increases the probability that at least one of the modules has a connection when changing between two cells. The lockout time describes the time (in milliseconds) within which a WLAN module does not perform any roaming operation or background scanning after the other WLAN module has successfully established a new connection.

Console path:

Setup > **WLAN** > **Dual-Roaming**

Possible values:

0 … 4294967295 Milliseconds

Default:

100

2.12.85 PMK caching

Manage PMK-caching here.

Console path:

Setup > **WLAN**

2.12.85.1 Default lifetime

Specifies the duration in seconds that the WLAN client stores the negotiated PMK.

Make sure that the time set here matches the session timeout in the accept message that the access point or RADIUS server sends to the WLAN client. Once this time has expired, the access point or RADIUS server requires a re-authentication.

Console path:

Setup > **WLAN** > **PMK-Caching**

Possible values:

0 … 4294967295 Milliseconds

Default:

0

Special values:

0

The negotiated PMK expires immediately.

2.12.85.2 Max.-Entries

Use this entry to specify how many entries are contained in the PMK cache.

Console path:

Setup > **WLAN** > **PMK-Caching**

Possible values:

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

Default:

4096

2.12.86 Paket-Capture

This menu contains the settings for packet capturing.

Console path:

Setup > **WLAN**

2.12.86.1 WLAN-Capture-Format

Using this setting you specify the format used by the packet capture function to store the WLAN-specific information in the capture file.

The selection of the appropriate capture format depends on the transmission standard in your WLAN network and the scope of the information that you would like to capture. The IEEE 802.11 standard with its numerous extensions has grown over many years. However, the capture formats that were developed in parallel are not flexible enough to cater optimally for every extension (particularly 802.11n). For this reason there is no universal capture format which is equally suitable for all standards. However, there are recommendations that cover a wide spectrum of standards: *Radiotap* and *PPI*.

Console path:

Setup > **WLAN** > **Packet-Capture**

Possible values:

Radiotap

Uses the radiotap header. Radiotap is a widely accepted format on Linux and BSD WLAN drivers which enables the creation of compact captures due to its flexible structure. With radiotap you can record a large amount of WLAN-specific information with a high compression rate. This also applies to data packets from 802.11n compliant connections. Limitations only arise when recording antenna-specific RSSI and signal strength as well as aggregations (A-MPDU). If you do not require detailed WLAN-specific information for this, choose the PPI format instead.

AVS

Uses the AVS header. The AVS header is a newer development of the PRISM header, and is used by LCOS as the standard header up to version 8.60. However, since AVS is also unable to process information from 802.11n compliant connections, you should choose the more powerful radiotap header.

PPI

Uses the Wireshark proprietary PPI header. Use this setting if you want to analyze the capture file with Wireshark. PPI offers similar functions as radiotap but can also bypass its limitations on the recording of information about 802.11n compliant connections. A disadvantage to radiotap is, however, the weaker compression and less detailed header structure.

PRISM

Uses the classic PRISM header. Only use this setting if you want to analyze the capture file with a program which does not support any of the other formats. PRISM is not suitable for recording information from 802.11n compliant connections. In the meantime this is considered obsolete and should no longer be used.

Plain

Disables all headers. Use this setting if you are only interested in the packet data itself.

Default:

Radiotap

2.12.87 Client Steering

This is where you specify the settings for the Client Management and the WLAN Band Steering for WLAN clients registered at the access point.

Console path:

Setup > **WLAN**

2.12.87.1 Operating

This option enables WLAN Band Steering or Client Management in the access point.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Client Management

Enables Client Management in the access point. The percentage settings given below refer to the maximum load of an access point. This is set to 80 clients and cannot be changed.

Radio-Band

Enables WLAN band steering in the access point.

No

Switches this feature off. With this setting, these features are managed by a WLC, for example.

Default:

No

2.12.87.3 Preferred-Band

Set here the preferred frequency band to which the access point steers the WLAN client.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

5GHz
2.4GHz

Default:

5GHz

2.12.87.4 Proberequest-Ageout-Seconds

Set the time (in seconds) that the WLAN client connection should be stored in the access point. When this time expires, the access point deletes the entry from the table.

This value should be set to a low value if you are using clients in the WLAN that frequently switch from dual-band to single-band mode.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

120

Special values:

0

The visible probe requests are deemed invalid immediately.

2.12.87.5 Initial-Blocktime-Seconds

When starting or restarting an access point with a 5 GHz DFS radio module and WLAN band steering activated, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a WLAN client to a preferred 5 GHz band. Instead, the 2.4 GHz radio module would answer the client request and forward it to the 2.4 GHz band.

By setting an initial block time, the radio module that is configured to 2.4 GHz only starts after the specified delay.

Registration of a purely 2.4 GHz WLAN client also occurs after this delay time. If no 5 GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Special values:

0

This value disables the delay.

Default:

10

2.12.87.6 Dry-Run

Client Management performs a test run. The scans are performed, decisions are calculated and logged, but not executed.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

2.12.87.7 Load-Recalculation-Interval

Interval in seconds, after which the load of the access point is calculated in Client Management. This results in the decision as to whether clients should be steered. If yes, then steering also takes place within this interval.

A higher value reduces the network load and has a limited positive effect in very large networks. A lower value leads to faster client steering. However, you should not go below 2 or above 10 seconds.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Special values:

0

This value disables the delay.

Default:

5

2.12.87.8 Load-Announcement-Delta

If Client Management detects a change in load that exceeds the specified percentage value, then messages outside of the usual interval report this load to the neighboring access points that were discovered by scan. The value should be increased in environments with many moving devices. The default of 5% (4 clients) is suitable for environments with few moving devices, e.g. in offices or classrooms.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

5

2.12.87.9 Load-Threshold

Percentage load threshold at which Client Management on an access point attempts to steer devices associated with it, irrespective of the load on neighboring access points. Increase the value in difficult environments with poor transmission quality or a high density of associated devices. In optimal environments with a high transmission quality and high throughput, such as in offices or classrooms, the load threshold can be reduced. The default of 80% (64 clients) lies between these extremes.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

80

2.12.87.10 Balancing-Difference

Relating to Client Management, this is the percentage difference in load between two neighboring access points, at which point the access point with the higher load attempts to steer clients to the access point with a lower load. A high value leads to an unbalanced scenario, while a low value leads to more steering attempts. If too many steering attempts are observed, this value should be increased. If a balanced scenario is a priority, then you have to reduce this value. The default of 10% (8 clients) difference should be suitable an office or classroom environment.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

10

2.12.87.11 Maximum-Neighbor-Count

Relating to Client Management, this is the number of neighboring access points taken into account for client steering and for the exchange of information between the access points. High-density environments benefit from a lower value, as clients can be steered to nearby access points with reduced communication between the access points. As a minimum you should consider 4 access points. The maximum is 72 access points, which is a limitation of the 802.11 protocol. Increasing the value to more than the default value of 20 produces no significant improvements.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

20

2.12.87.12 Neighbor-Signal-Threshold

Signal strength in dBm at which Client Management classifies an access point as a neighbor. Lower values (-80, -90) are useful for networks that cover a wider area. Higher values (-60, -50) are useful in high-density environments.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

-70

2.12.87.13 Legacy-Steering

Normally, Client Management only attempts to steer clients to a different access point that correctly supports the 802.11v protocol. If you set this parameter to "Yes" then steering is attempted for every client. During a steering event, the client is denied access to the access point for a period. The intention is to force it to switch to another access point. From the user's perspective, the WLAN simply appears to be gone for a while.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

2.12.87.14 Minimal-Load-Difference

Relating to Client Management, this is the minimum percentage load difference between access points at which client steering takes place. Only applies if the load threshold is exceeded. Should not be set to a larger value than "Balancing-Difference" as the calculations could be incorrect. Also, no lower than 2%, otherwise there is a risk that a client is moved back and forth between two access points.

A low value results in more steering events in high-load environments. This may be useful in environments where the clients are relatively stationary. A high value results in fewer steering events, which is useful in environments with high loads and numerous mobile clients.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

5

2.12.87.15 Daily-Env-Scan-Hour

Time at which an environment scan is performed when Client Management is enabled. The scan is performed at random within a 30-minute time window to minimize the chance of access points conflicting. A scan takes about 15 seconds with "Scan-Period" in the default setting. The access point is unavailable to clients throughout the scan, so the least possible number of clients should be active at the selected time. The default is 3 o'clock in the morning.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

0 … 23

Default:

3

2.12.87.16 Scan-Period

Time in milliseconds that the client-management environment scan searches for other access points on a given channel. This should be 2 to 2.5 times your own beacon interval. The default value works with a common beacon interval. Higher values are only necessary with higher beacon intervals, although this increases the risk of scan conflicts when the access point is starting or during the nightly scans.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

200 … 1000

Default:

400

2.12.87.17 AP-Steering-RSSI-Threshold

The signal strength in dBm that a client must have on a remote access point in order to be directed to it by Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

-75

2.12.87.18 Remote-Station-Expiration

Time in seconds for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions made by the Client Management. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

600

2.12.87.19 Blacklist-Clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering. Either explicitly or via wildcards. This provides the best user experience for compatible clients without affecting incompatible clients.

Console path:

Setup > **WLAN** > **Client-Steering**

2.12.87.19.1 MAC address

The MAC addresses of the clients to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

Console path:

Setup > **WLAN** > **Client-Steering** > **Blacklist-Clients**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.12.87.20 Start-Environment-Scan

This action manually starts the Client Management environment scan. This can be used if new access points have been added and they are not yet visible in the table of neighboring access points. Start the action using `do Start-Environment-Scan`.

Console path:

Setup > **WLAN** > **Client-Steering**

2.12.87.21 Client Management mode

Client Management operating mode. You can choose either to steer the clients between access points only or to additionally use band steering, which optimizes the frequency bands used by each access point.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

AP-Steering
AP+Band-Steering

Default:

AP+Band-Steering

2.12.87.22 Band-Ratio

Ratio of distribution between bands in percent. This is used for the band-steering feature of Client Management.

The ratio indicates how many 5 GHz clients are able to connect to this access point. If more clients are connected at 5 GHz, clients are steered to 2.4 GHz. If more clients are connected at 2.4 GHz, clients are steered to 5 GHz.

Decrease the percentage if you are working with a channel width of 20 MHz in the 5 GHz band and your 2.4 GHz spectrum is free, i.e. there are few conflicting SSIDs and few other users such as Bluetooth. Choose a higher ratio if your 2.4 GHz band is full.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

75

2.12.87.23 Band-Steering-RSSI-Threshold

Signal strength in dBm that a client must have on the other band in order for it to be steered. This is used for the band-steering feature of Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to a band with a poor signal quality. Clients may even refuse to be steered to a band with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the band.

The default value is ideal for office environments.

Console path:

Setup > **WLAN** > **Client-Steering**

Possible values:

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

Default:

-65

2.12.89 Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

Console path:

Setup > **WLAN**

2.12.89.1 MAC address pattern

Enter the MAC address of a station.

It is possible to use wildcards.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Possible arguments:

MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

It is possible to use wildcards.

2.12.89.2 Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

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

2.12.89.3 Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

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

2.12.89.4 WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

This field has no significance for networks secured by WEP.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

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

2.12.89.5 Tx-Limit

A LANCOM Access Point in client mode communicates its setting to the Access Point when logging on. This then uses uses these two values to set the minimum bandwidth as restriction.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an Access Point Rx stands for “Send data” and Tx stands for “Receive data”.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

2.12.89.6 Rx-Limit

A LANCOM Access Point in client mode communicates its setting to the Access Point when logging on. This then uses uses these two values to set the minimum bandwidth as restriction.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an Access Point Rx stands for “Send data” and Tx stands for “Receive data”.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

2.12.89.7 VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here. Consequently the client can only be reached by packets originating from the same VLAN. Packets sent by the client are marked with this VLAN ID. You only need to set this value if you want this client to belong to a different VLAN than the

logical WLAN (SSID) that it is connected to. 0 means that the client belongs to the VLAN of its logical WLAN (SSID), if this belongs to a VLAN at all.

If you use IPv6, or if multicast is operating on a VLAN, different group keys must be assigned to the different VLANs of an SSID. Otherwise the different multicasts are not be assigned to the correct clients. When using IPv6, for example, clients are informed of IPv6 prefixes that do not function on the VLAN ID.

Console path:

Setup > **WLAN** > **Access-Rules**

Possible values:

Max. 4 characters from `0123456789`

0 … 4096

Default:

0

Special values:

0

No limit

2.12.89.9 SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.

The use of wildcards makes it possible to allow access to multiple SSIDs.

Console path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Special values:

*****

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

empty

2.12.100 Card-Reinit-Cycle

In this interval (in seconds) the internal WLAN cards in older access points are reinitialized in order to keep point-to-point connections active. This function is handled by the "alive test" in newer models.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

0

Special values:

0

Deactivates this function.

2.12.101 Noise-Calibration-Cycle

WLAN cards fitted with the Atheros chipset measure noise levels on the medium in this interval (in seconds).

Console path:

Setup > **WLAN**

Possible values:

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

Default:

0

Special values:

0

Deactivates this function.

2.12.103 Trace-MAC

The output of trace messages for the WLAN-Data-Trace can be set for a certain client. The corresponding MAC address is entered here.

Console path:

Setup > **WLAN**

Possible values:

Max. 12 characters from `[A-F][0-9]`

Default:

000000000000

Special values:

000000000000

Deactivates this function and outputs trace messages for all clients.

2.12.105 Therm.-Recal.-Cycle

In this interval (in seconds) WLAN cards fitted with the Atheros chipset adjust their transmission power to compensate for thermal variations.

Please note that deactivating the thermal recalibration cycle for these cards means that they cannot react to changes in temperature.

Console path:

Setup > **WLAN**

Possible values:

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

Default:

20

Special values:

0

Deactivates this function.

2.12.109 Noise offsets

This table is used to define the correction factors which adjust the displayed signal values.

Console path:

Setup > **WLAN**

2.12.109.1 Band

This table is used to define the correction factors which adjust the displayed signal values.

Console path:

Setup > **WLAN** > **Noise-Offsets**

Possible values:

5GHz
2.4GHz

Default:

2.4GHz

2.12.109.2 Channel

The noise-offset value is applied to the channel selected here.

Console path:

Setup > **WLAN** > **Noise-Offsets**

Possible values:

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

Default:

empty

2.12.109.3 Interface

The noise-offset value is applied to the WLAN interface selected here.

Console path:

Setup > **WLAN** > **Noise-Offsets**

Possible values:

Depend on the hardware capabilities, e.g. WLAN-1 or WLAN-2
WLAN-1

Default:

WLAN-1

2.12.109.4 Value

This numeric value is added to the current noise value.

Console path:

Setup > **WLAN** > **Noise-Offsets**

Possible values:

0 … 127

Default:

10

2.12.110 Trace level

The output of trace messages for the WLAN data trace can be restricted to contain certain content only. The messages are entered in the form of a bit mask for this.

Console path:

Setup > **WLAN**

Possible values:

0 to 255

0

Reports that a packet has been received/sent.

1

Adds the physical parameters for the packets (data rate, signal strength…).

2

Adds the MAC header.

3

Adds the Layer-3 header (e.g. IP/IPX).

4

Adds the Layer-4 header (TCP, UDP…).

5

Adds the TCP/UDP payload.

255

Default:

255

2.12.111 Noise immunity

The settings for noise-immunity (Adaptive Noise Immunity - ANI) can be adjusted here.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN**

2.12.111.1 Noise immunity

This item sets the threshold value to be used for noise immunity.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.111.2 OFDM-Weak-Signal-Detection

This item sets the threshold value to be used for detecting weak OFDM signals.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.111.3 CCK-Weak-Signal-Detection-Threshold

This item sets the threshold value to be used for detecting weak CCK signals.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.111.4 Fir step level

This item sets the value to be used for the fir step.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.111.5 Spurious immunity level

This item sets the value to be used for the fir step.

Under most conditions the settings for noise immunity are controlled automatically by the WLAN module driver according to the radio-field conditions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.111.6 MRC-CCK

With this parameter, the Maximum Ratio Combining (MRC) for 802.11b rates (1 to 11 Mbit) on devices with an Osprey WLAN module (AR93xx) can be enabled (value != `0`) or disabled (value = `0`). The default value `255` means that the WLAN driver presetting is not overridden. In certain cases it may be reasonable to set this value to `0` in order to artificially "deafen" the receiver in the device.

Console path:

Setup > **WLAN** > **Noise-Immunity**

Possible values:

0 … 255

Default:

255

2.12.114 Aggregate-Retry-Limit

This parameter specifies how many times a set of packets to be sent by the hardware may be repeated until it is deferred while other packets waiting to be sent are transmitted. Restricting the number of repeat attempts to a small amount, e.g. in VoIP environments, limits the maximum delay for VoIP packets

The absolute value set under "Hard-Retries" for transmission attempts remains unaffected by the setting here.

Console path:

Setup > **WLAN**

Possible values:

0 … 255

Default:

255

2.12.115 Omit-Global-Crypto-Sequence-Check

This is where you set the value for the crypto sequence check.

Console path:

Setup > **WLAN**

Possible values:

Auto

LCOS contains a list of relevant devices. In the "Auto" setting, the global sequence check is disabled. For other devices not included in this list, the global sequence check has to be disabled manually.

Yes

No

Default:

Auto

2.12.116 Trace packets

Similar to Trace MAC and Trace level, the output from WLAN DATA traces can be restricted by the type of packet sent or received, e.g. management (authenticate, association, action, probe-request/response), control (e.g. powersave poll), EAPOL (802.1x negotiation, WPA key handshake).

Console path:

Setup > **WLAN**

Possible values:

One or more values from Management, Control, Data, EAPOL, All

All

Default:

All

2.12.117 WPA-Handshake-Delay-ms

This setting sets the time (in milliseconds) that the device delays the WPA handshake when roaming. A value of 0 means that there is no delay.

Console path:

Setup > **WLAN**

Possible values:

0 … 4294967295 Milliseconds

Default:

0

2.12.118 WPA-Handshake-Timeout-Override-ms

This setting sets the time (in milliseconds) that the device overrides the WPA handshake timeout when roaming. A value of 0 means that there is no override.

Console path:

Setup > **WLAN**

Possible values:

0 … 4294967295 Milliseconds

Default:

0

2.12.120 Rx-Aggregate-Flush-Timeout-ms

Using this setting you determine the time (in milliseconds) after which the device views parts of aggregates that were not received as "lost", and the subsequent packets are no longer retained.

Console path:

Setup > **WLAN**

Possible values:

0 … 4294967295 Milliseconds

Default:

40

2.12.123 Aggregate-Time-Limit-us

Console path:

Setup > **WLAN**

Possible values:

0 … 4294967295 Microseconds

Default:

40

2.12.124 Trace-Mgmt-Packets

With this selection it is possible to set which type of management frames should automatically appear in the WLAN-DATA trace

Console path:

Setup > **WLAN**

Possible values:

Association
(Re)association request/response
Disassociate
Authentication
Authentication
Deauthentication
Probes
Probe request
Probe response
Action
Beacon
Other
All other management frame types

Default:

Association

Authentication

Probes

Action

Other

2.12.125 Trace-Data-Packets

With this selection it is possible to set which type of data frames should automatically appear in the WLAN-DATA trace

Console path:

Setup > **WLAN**

Possible values:

Normal
All normal data packets
NULL
All empty data packets
Other
All other data packets

2.12.126 Trace-Tx-Complete-with-Packet

With this selection it is possible to set which type of TX complete frames should automatically appear in the WLAN-DATA trace

Console path:

Setup > **WLAN**

2.12.130 DFS

This menu is used to configure the Dynamic Frequency Selection (DFS). DFS enables an access point to change channels if another system, such as such as a weather radar, should become active on the current channel.

Console path:

Setup > **WLAN**

2.12.130.1 Use-Full-Channelset

When 5 GHz and DFS are operated and you are operating DFS according to EN 301893-1.3 or earlier, this parameter allows the use of channels 120, 124, 128, which are otherwise blocked for weather radar. EN 301893 currently does not support these channels; this parameter has no effect.

Please not that activating this option constitutes a breach of ETSI regulations because no approval has been granted for LCOS.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No

The access point ignores channels 120, 124 and 128 when changing the channel.

Yes

The access point includes channels 120, 124 and 128 when changing the channel.

Default:

No

2.12.130.2 Radar-Load-Threshold

This value indicates the percentage utilization of the WLAN module at which the access point reduces the accuracy of radar detection.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

Max. 3 characters from `0123456789`

0 … 100 Percent

Default:

80

2.12.130.3 Direct-Channelswitching

Use this parameter to determine how the device performs the channel availability check (CAC) as required by DFS.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No

The device observes a randomly selected channel (country-specific choice) for at least 60 seconds to see if it is free of radar before broadcasting on this channel. In order to be able to quickly change channel if radar is detected during operations, the device determines a minimum number of alternative channels that are expected to be vacant (also see *2.23.20.8.27 DFS-Rescan-Num-Channels* on page 760.

Yes

Within a period of 60 seconds, the device gathers information about all of the channels by jumping between them at 500ms intervals. If the device subsequently detects a radar during its operations, it immediately switches to another channel.

Note that this mode currently no longer complies with the approval, so the switch is disabled by default.

Default:

No

2.12.130.4 DFS test mode

You enable or disable the DFS test mode with this setting. If it is enabled, the device only reports known radar bursts and does not switch radio channels – contrary to normal operation.

This parameter is required exclusively for development tests and is not relevant for normal operations. Never change this default setting!

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No

The DFS test mode is disabled.

Yes

The DFS test mode is enabled.

Default:

No

2.12.130.5 Ignore CRC errors

With this parameter you specify whether the device ignores radar pulses that are reported by the system at the same time as a CRC error.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No
Yes

Default:

Yes

2.12.130.6 Trace ignored pulses

This parameter specifies whether LCOS conducting the DFS pulse trace reports radar pulses that are reported by the WLAN hardware but are rejected by the software as being invalid.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No
Yes

Default:

No

2.12.130.7 Go for highest bandwidth

This parameter specifies whether the device selects the channels that offer the highest bandwidth, assuming that the eligible channels are stored as radar-free.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No

The device will start operating immediately, although with a reduced channel bandwidth (e.g. 20 instead of 40 MHz).

Yes

The device initially performs a channel availability check to find groups of channels that support operations at the full or at least with an increased channel bandwidth.

Default:

Yes

2.12.130.8 Prefer fast switch

This parameter is a placeholder and currently has no function.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

No
Yes

Default:

Yes

2.12.130.9 Channel change delay

Here you specify how long an access point, which has detected a radar, waits until it changes to a different channel.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

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

Default:

0

Special values:

0

The value 0 disables this function.

2.12.130.10 Radar-Pattern-Thresholds

In this table, you specify the threshold values for radar detection.

Console path:

Setup > **WLAN** > **DFS**

2.12.130.10.1 Pattern-pps

Select one of the predefined radar patterns here to change the threshold value for the radar pattern recognition.

Console path:

Setup > **WLAN** > **DFS** > **Radar-Pattern-Thresholds**

Possible values:

Pattern-pps

EN301893-1.2-700pps
EN301893-1.2-1800pps
EN301893-1.2-330pps
EN301893-1.3-750pps
EN301893-1.3-200pps
EN301893-1.3-300pps
EN301893-1.3-500pps
EN301893-1.3-800pps
EN301893-1.3-1000pps
EN301893-1.3-1200pps
EN301893-1.3-1500pps
EN301893-1.3-1600pps
EN301893-1.3-2000pps
EN301893-1.3-2300pps
EN301893-1.3-3000pps
EN301893-1.3-3500pps
EN301893-1.3-4000pps
EN302502-200pps
EN302502-300pps
EN302502-500pps
EN302502-750pps
EN302502-800pps
EN302502-1000pps
EN302502-1200pps
EN302502-1500pps
EN302502-1600pps
EN302502-2000pps
EN302502-2300pps
EN302502-3000pps
EN302502-3500pps
EN302502-4000pps

EN302502-4500pps

2.12.130.10.2 Threshold

The value entered here describes the accuracy with which the corresponding radar pattern is detected.

Changing these default values may cause the device to operate in violation of the standard ETSI EN 301 893 version 1.3.

Console path:

Setup > **WLAN** > **DFS** > **Radar-Pattern-Thresholds**

Possible values:

0 … 4294967295

Default:

depending on the selected radar pattern

2.12.130.11 Min.-internal-Channel-Distance

Use this entry to specify the internal minimum channel distance for DFS.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

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

Default:

0

2.12.130.15 CAC-Time-5.6GHz

Time of the channel availability check. With this setting you specify how long (in seconds) a WLAN module operating DFS carries out the initial check of the 5.6 GHz channels before it selects a radio channel and starts transmitting data.

The duration of the channel availability check is regulated by applicable standards (e.g. in Europe by the ETSI EN 301 893). Please observe the regulations valid for your country.

Console path:

Setup > **WLAN** > **DFS**

Possible values:

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

Default:

empty

2.12.131 RTLS

This menu contains the settings for communications with an RTLS server.

Console path:

Setup > **WLAN**

2.12.131.4 Ekahau

This menu contains the settings for the AiRISTA Flow blink mode (formerly Ekahau blink mode).

Console path:

Setup > **WLAN** > **RTLS**

2.12.131.4.1 Server-Address

Contains the IP address or the DNS name of the RTLS server.

Console path:

Setup > **WLAN** > **RTLS** > **Ekahau**

Possible values:

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

Default:

empty

2.12.131.4.2 Server-Port

Contains the UDP port number of the RTLS server.

Console path:

Setup > **WLAN** > **RTLS** > **Ekahau**

Possible values:

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

Default:

8569

2.12.131.4.3 Loopback-Address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

Console path:

Setup > **WLAN** > **RTLS** > **Ekahau**

Possible values:

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

Special values:

Name of the IP networks whose address should be used

"INT"

for the address of the first intranet

"DMZ"

for the address of the first DMZ

LB0 to LBF

for the 16 loopback addresses

Any valid IP address

Default:

empty

2.12.131.5 AeroScout

This menu contains the Stanley AeroScout RTLS settings.

Console path:

Setup > **WLAN** > **RTLS**

2.12.131.5.1 Server-Address

Contains the IP address or the DNS name of the RTLS server.

Console path:

Setup > **WLAN** > **RTLS** > **AeroScout**

Possible values:

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

Default:

empty

2.12.131.5.2 Server-Port

Contains the server port of the AeroScout Location Engine.

Console path:

Setup > **WLAN** > **RTLS** > **AeroScout**

Possible values:

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

Default:

12092

2.12.131.5.3 Loopback-Address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

Console path:

Setup > **WLAN** > **RTLS** > **AeroScout**

Possible values:

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

Special values:

Name of the IP networks whose address should be used

"INT"

for the address of the first intranet

"DMZ"

for the address of the first DMZ

LB0 to LBF

for the 16 loopback addresses

Any valid IP address

Default:

empty

2.12.131.5.4 Operating

Enable the forwarding to the Aeroscout Location Engine here.

Console path:

Setup > **WLAN** > **RTLS** > **AeroScout**

Possible values:

Yes

Forwarding enabled.

No

Default:

No

2.12.131.5.5 Vendor-ID

Here you configure the vendor ID that the access point reports to the AeroScout Location Engine. If your version of the Aeroscout Location Engine does not yet support the dedicated LANCOM vendor ID, you can switch to the "Motorola" vendor ID.

Console path:

Setup > **WLAN** > **RTLS** > **AeroScout**

Possible values:

Motorola
LANCOM

Default:

LANCOM

2.12.132 Roaming-Targets

With Client Management enabled, the table under `/Status/WLAN/Roaming-Targets` is filled out automatically.

Additionally, any targets added manually to this table are also included in the list of neighbors in an 802.11k advertisement, even if they are out of range. The number of automatically added roaming targets is limited by *2.12.87.11 Maximum-Neighbor-Count* on page 425.

Console path:

Setup > **WLAN**

2.12.132.1 Name

As a part of client management, the names of the roaming targets for this access point are entered here after an environment scan. This is a part of the standard IEEE 802.11k. This standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the WLAN client in the "Neighbor Report" as defined for the standard.

Client management makes these entries automatically. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately. In this case, you enter the device names of the potential roaming targets here, i.e. other access points of the same SSID.

The device name is used so that further required information about the potential roaming target (e.g. the channel number) can be communicated via IAAP. For this reason it is necessary for the participating access points to communicate with one another via IAPP.

Depending on the scenario, it may be desirable for a dual-radio access point to communicate its own, second WLAN module as a potential roaming target. In this case, the device's own name can also be entered into the table.

Console path:

Setup > **WLAN** > **Roaming-Target**

Possible values:

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

2.12.133 LEPS-U

LANCOM Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

Console path:

Setup > **WLAN**

2.12.133.1 Operating

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

Console path:

Setup > **WLAN** > **LEPS-U**

Possible values:

No
Yes

Default:

No

2.12.133.2 Profiles

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

Console path:

Setup > **WLAN** > **LEPS-U**

2.12.133.2.1 Name

Enter a unique name for the LEPS-U profile here.

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

2.12.133.2.2 Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. 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-U profile.

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

2.12.133.2.3 Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Special values:

0

No limit.

2.12.133.2.4 Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Special values:

0

No limit.

2.12.133.2.5 VLAN-ID

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

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

2.12.133.3 Users

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

Console path:

Setup > **WLAN** > **LEPS-U**

2.12.133.3.1 Name

Enter a unique name for the LEPS-U user here.

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

2.12.133.3.2 Profile

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

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

2.12.133.3.3 WPA passphrase

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

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

2.12.133.3.4 Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0–9]`

Special values:

0

No limit.

2.12.133.3.5 Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0–9]`

Special values:

0

No limit.

2.12.133.3.6 VLAN-ID

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

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0–9]`

2.12.134 QoS

Use this menu to specify a QoS map set.

Console path:

Setup > **WLAN**

2.12.134.1 QoS-Map-Source

Set one of the predefined QoS map sets here.

Console path:

Setup > **WLAN** > **QoS**

Possible values:

LAN-Config
Standard QoS map of the LCOS.

ID1
One of the QoS maps predefined by the Wi-Fi Alliance.

ID2
One of the QoS maps predefined by the Wi-Fi Alliance.

Default:

LAN-Config

2.12.135 Hotspot2.0

Use this menu to adjust settings that are specific to HotSpot 2.0/Passpoint.

Console path:

Setup > **WLAN**

2.12.135.1 Check-Release

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

Console path:

Setup > **WLAN** > **Hotspot2.0**

Possible values:

Yes
Off

Default:

Yes

2.12.136 ARP-Handling-Settings

The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. In most cases an alternative is to suppress broadcasts/multicasts by using *Transmit-only-Unicasts*.

Console path:

Setup > **WLAN**

2.12.136.2 Unknown-Address-Action

In case of an unknown address, the packet is either forwarded or discarded.

Console path:

Setup > **WLAN** > **ARP-Handling-Settings**

Possible values:

Forward
Discard

Default:

Forward

2.12.136.3 Broadcast-Response-Action

In case of a broadcast, the packet is either forwarded or discarded.

Console path:

Setup > **WLAN** > **ARP-Handling-Settings**

Possible values:

Forward
Discard

Default:

Forward

2.12.141 Send-Mails

Determines whether notifications about WLAN events are sent to the e-mail address specified in 2.12.41 .

Console path:

Setup > **WLAN**

Possible values:

No
Yes

Default:

No

2.12.248 Wireless-IDS

The Wireless Intrusion Detection System (Wireless IDS) provides APs with the ability to detect potential intrusion attacks and provide warnings to the network management software when the attack activities exceed the corresponding user-defined threshold value/interval.

Console path:

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

2.12.248.9 IDS-Operational

Enable or disable Wireless IDS here.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

No

Wireless IDS disabled

Yes

Wireless IDS enabled

Default:

No

2.12.248.10 Syslog-Operational

Enable or disable the creation of syslog entries via Wireless IDS here.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

No

Creation of syslog entries via Wireless IDS disabled

Yes

Creation of syslog entries via Wireless IDS enabled

Default:

Yes

2.12.248.11 SNMPTraps-Operational

Enable or disable the sending of traps via Wireless IDS.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

No

Sending traps via Wireless IDS disabled

Yes

Sending traps via Wireless IDS enabled

Default:

No

2.12.248.12 E-Mail

Enable or disable e-mail notifications via Wireless IDS here.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

No

E-mail notifications via Wireless IDS disabled

Yes

E-mail notifications via Wireless IDS enabled

Default:

No

2.12.248.13 E-Mail-Receiver

Specify the e-mail destination address here.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

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

2.12.248.14 E-Mail-Aggregate-Interval

Here you specify the period of time between the initial receipt of a Wireless IDS event and the e-mail being sent. This functions helps to prevent a flood of attacks causing an e-mail flood.

Console path:

Setup > **WLAN** > **Wireless-IDS**

Possible values:

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

Special values:

0

E-mail sending for each event

Default:

10

2.12.248.50 Signatures

Here you configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

Console path:

Setup > **WLAN** > **Wireless-IDS**

2.12.248.50.1 AssociateReqFlood

Here you configure the threshold for attacks of the type AssociateReqFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.1.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

Possible values:

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

Default:

250

2.12.248.50.1.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

Possible values:

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

Default:

10

2.12.248.50.2 ReassociateReqFlood

Here you configure the threshold for attacks of the type ReassociateReqFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.2.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

Possible values:

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

Default:

250

2.12.248.50.2.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

Possible values:

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

Default:

10

2.12.248.50.3 AuthenticateReqFlood

Here you configure the threshold for attacks of the type AuthenticateReqFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.3.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

Possible values:

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

Default:

250

2.12.248.50.3.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

Possible values:

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

Default:

10

2.12.248.50.4 EAPOLStart

Here you configure the threshold for attacks of the type EAPOLStart.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.4.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

Possible values:

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

Default:

250

2.12.248.50.4.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

Possible values:

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

Default:

10

2.12.248.50.5 ProbeBroadcast

Here you configure the threshold for attacks of the type ProbeBroadcast.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.5.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

Possible values:

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

Default:

1500

2.12.248.50.5.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

Possible values:

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

Default:

10

2.12.248.50.6 DisassociateBroadcast

Here you configure the threshold for attacks of the type DisassociateBroadcast.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.6.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

Possible values:

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

Default:

2

2.12.248.50.6.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

Possible values:

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

Default:

1

2.12.248.50.7 DeauthenticateBroadcast

Here you configure the threshold for attacks of the type DeauthenticateBroadcast.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.7.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

Possible values:

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

Default:

2

2.12.248.50.7.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

Possible values:

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

Default:

1

2.12.248.50.8 DisassociateReqFlood

Here you configure the threshold for attacks of the type DisassociateReqFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.8.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

Possible values:

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

Default:

250

2.12.248.50.8.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

Possible values:

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

Default:

10

2.12.248.50.9 BlockAckOutOfWindow

Here you configure the threshold for attacks of the type BlockAckOutOfWindow.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.9.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

Possible values:

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

Default:

200

2.12.248.50.9.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

Possible values:

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

Default:

5

2.12.248.50.10 BlockAckAfterDelBA

Here you configure the threshold for attacks of the type BlockAckAfterDelBA.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.10.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

Possible values:

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

Default:

100

2.12.248.50.10.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

Possible values:

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

Default:

5

2.12.248.50.11 NullDataFlood

Here you configure the threshold for attacks of the type NullDataFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.11.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

Possible values:

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

Default:

500

2.12.248.50.11.2 CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

Possible values:

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

Default:

5

2.12.248.50.12 NullDataPSBufferOverflow

Here you configure the threshold for attacks of the type NullDataPSBufferOverflow.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.12.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

Possible values:

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

Default:

200

2.12.248.50.12.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

Possible values:

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

Default:

5

2.12.248.50.13 PSPollTIMInterval

Here you configure the threshold for attacks of the type PSPollTIMInterval.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.13.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

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

Default:

100

2.12.248.50.13.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

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

Default:

5

2.12.248.50.13.3 Interval-Diff

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

Possible values:

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

Default:

5

2.12.248.50.14 SMPSMUltiStream

Here you configure the threshold for attacks of the type SMPSMUltiStream.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.14.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMUltiStream**

Possible values:

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

Default:

100

2.12.248.50.14.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMUltiStream**

Possible values:

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

Default:

5

2.12.248.50.15 DeauthenticateReqFlood

Here you configure the threshold for attacks of the type DeauthenticateReqFlood.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.15.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

Possible values:

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

Default:

250

2.12.248.50.15.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

Possible values:

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

Default:

10

2.12.248.50.16 PrematureEAPOLSuccess

Here you configure the threshold for attacks of the type PrematureEAPOLSuccess.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.16.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLSuccess**

Possible values:

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

Default:

2

2.12.248.50.16.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLSuccess**

Possible values:

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

Default:

1

2.12.248.50.17 PrematureEAPOLFailure

Here you configure the threshold for attacks of the type PrematureEAPOLFailure.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

2.12.248.50.17.1 CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLFailure**

Possible values:

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

Default:

2

2.12.248.50.17.2 CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures** > **PrematureEAPOLFailure**

Possible values:

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

Default:

1

2.12.248.51 Promiscuous-Mode

Activates or deactivates the promiscuous mode. This mode handles also packets that were not sent to the device itself. These packets are forwarded to LCOS to allow an analysis by the WIDS.

This mode can be used to detect the following attacks:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess
- DeauthenticateReqFlood
- DisassociateReqFlood

Please note that the promiscuous mode has a significant impact on the performance. For example, frame aggregation is deactivated while it is in action. Only use this mode in case of a strong suspicion.

Console path:

Setup > **WLAN** > **Wireless-IDS** > **Signatures**

Possible values:

No

Promiscuous mode is disabled.

Yes

Promiscuous mode is enabled.

Default:

No

2.14 Time

This menu contains the configuration of the device time settings.

Console path:

Setup

2.14.1 Fetch method

Select here if and how the device synchronizes its internal real-time clock.

Console path:

Setup > **Time**

Possible values:

None
NTP
GPS

Default:

NTP

2.14.2 Current time

Display of current time.

Console path:

Setup > **Time**

2.14.7 UTC in seconds

This parameter is used by LANmonitor to read the time.

Console path:

Setup > **Time**

2.14.10 Time zone

This item sets the timezone for the location of your device. The time zone is the difference between local time and Coordinated Universal Time (UTC) in hours. This is especially important for the Network Time Protocol (NTP)

Console path:

Setup > **Time**

Possible values:

+1
+2…+14
-1…-12

Default:

+1

2.14.11 Daylight-saving time

The time change between local standard time and daylight-saving time can be set here manually or automatically. For automatic daylight saving time adjustment, enter the appropriate time region for the location of your device. If your device is located outside the specified time regions, the use of automatic time adjustment requires you to select 'User defined' and for you to enter the following values into the table for automatic time adjustment.

Console path:

Setup > **Time**

Possible values:

Yes
No
Europe (EU)
Russia
USA
Userdefined

Default:

Europe (EU)

2.14.12 DST clock changes

Here you configure the individual values for the automatic clock change between summer and winter time, assuming that the local daylight-saving time settings have been selected as "User defined".

Console path:

Setup > **Time**

2.14.12.1 Event

Defines the beginning and end of daylight saving time.

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.2 Index

First or last day of month for switching to daylight-saving time (summertime).

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.3 Day

Defines on which recurring weekday of the month the time change is carried out.

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.4 Month

The month in which the change is carried out.

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.5 Hour

The hour at which the change is carried out.

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.6 Minute

The minute at which the change is carried out.

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.12.7 Time type

Time standard, such as UTC (Coordinated Universal Time).

Console path:

Setup > **Time** > **DST-clock-changes**

2.14.13 Get time

This command causes the device to fetch the current time from the specified time server.

Console path:

Setup > **Time**

2.14.15 Holidays

This table contains the holidays that have been defined.

Console path:

Setup > **Time**

2.14.15.1 Index

This describes the position of the entry in the table.

Console path:

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

Possible values:

0 … 9999

Default:

empty

2.14.15.2 Date

If you have created entries in the timed control table that should apply on public holidays, enter the days here.

Console path:

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

Possible values:

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

Default:

empty

2.14.16 Timeframe

Timeframes are used to define the periods when the content-filter profiles are valid. One profile may contain several lines with different timeframes. Different lines in a timeframe should complement one another, i.e. if you specify WORKTIME you will should probably specify a timeframe called FREETIME to cover the time outside of working hours.

Console path:

Setup > **Time**

2.14.16.1 Name

Enter the name of the timeframe for referencing from the content-filter profile.

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** > **Timeframe**

Possible values:

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

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 from HH:MM normally goes to HH:MM:00, with the exception of stop time 00:00, which is interpreted as 23:59:59.

Console path:

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

Possible values:

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

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** > **Timeframe**

Possible values:

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

Default:

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

2.17 DNS

This menu contains the domain-name system (DNS) configuration.

Console path:

Setup

2.17.1 Operating

Activates or deactivates DNS.

Console path:

Setup > **DNS**

Possible values:

Yes
No

Default:

Yes

2.17.2 Domain

Device's own domain.

Console path:

Setup > **DNS**

Possible values:

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

Default:

Internal

2.17.3 DHCP usage

The DNS server can resolve the names of the stations that have requested an IP address by DHCP.

Use this switch to activate this option.

Console path:

Setup > **DNS**

Possible values:

Yes
No

Default:

Yes

2.17.5 DNS-List

Enter the station names and the associated IP addresses here.

Console path:

Setup > **DNS**

2.17.5.1 Host name

Enter the name of a station here.

For example, if you have a computer named `myhost` and your domain name is `myhome.internal`, then you should enter the station name here as `myhost.myhome.intern`.

Console path:

Setup > **DNS** > **DNS-List**

Possible values:

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

Default:

empty

2.17.5.2 IP address

Enter the valid IP address of the station.

If a client needs to resolve the name of a station, it sends a request with that name to the DNS server. The server responds by communicating the IP address entered here.

Console path:

Setup > **DNS** > **DNS-List**

Possible values:

Max. 64 characters from `[0-9].`

Default:

0.0.0.0

2.17.5.3 IPv6 address

Enter the valid IPv6 address of the station.

If a client needs to resolve the name of a station, it sends a request with that name to the DNS server. The server responds by communicating the IPv6 address entered here.

Console path:

Setup > **DNS** > **DNS-List**

Possible values:

Max. 64 characters from `[0-9].`

Default:

empty

2.17.5.4 Rtg-Tag

When resolving a station name, the device uses the routing tag to set the tag context for that station.

Console path:

Setup > **DNS** > **DNS-List**

Possible values:

0 … 65535

Default:

0

2.17.6 Filter-List

Use the DNS filter to block access to certain stations or domains.

Console path:

Setup > **DNS**

2.17.6.1 Idx.

Index for the filter entries.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

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

Default:

empty

2.17.6.2 Domain

Enter the name of a station or a domain that you want to block. The characters "*" and "?" can be used as wildcards.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

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

Default:

empty

2.17.6.3 IP-Address

If you want this access restriction to only apply to a specific workstation or subnetwork, enter the valid IP address of the workstation or subnetwork here.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.17.6.4 Netmask

If you have entered the address of a subnetwork for access restriction, you must enter the associated subnet mask here.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.17.6.5 IPv6-Prefix

Using this setting you set the IPv6 sender addresses for which the device filters the domain. If you want to apply the filter to all IPv6 addresses, select the prefix `::/0`.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

Max. 43 characters from `[a-z][0-9]/:`

Default:

empty

2.17.6.6 Rtg-tag

The routing tag determines which filters apply in each tag context.

Console path:

Setup > **DNS** > **Filter-List**

Possible values:

0 … 65535

Default:

0

2.17.7 Lease time

Some computers store the names and addresses of clients that they have queried from a DNS server in order to be able to access this information more quickly in the future.

Specify here how long this data may be stored before becoming invalid. After this time the computer in question must issue a new request for the information.

Console path:

Setup > **DNS**

Possible values:

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

Default:

2000

2.17.8 Dyn.-DNS-List

The Dyn DNS list records names that were registered via a register request. Windows does this when, for example, under Advanced TCP/IP Settings, "DNS", the network-connection options "Register this connection's addresses in DNS" and "Use this connection's DNS suffix in DNS registration" have been activated and the stations register in the domain.

Console path:

Setup > **DNS**

2.17.8.1 Host name

Name of the station that registered via a register request.

Console path:

Setup > **DNS** > **Dyn.-DNS-List**

2.17.8.2 IP address

Valid IP address of the station that registered via a register request.

Console path:

Setup > **DNS** > **Dyn.-DNS-List**

2.17.8.3 Timeout

Lease period for this entry.

Console path:

Setup > **DNS** > **Dyn.-DNS-List**

2.17.8.4 IPv6 address

Displays the IPv6 address of the corresponding host (if available).

Console path:

Setup > **DNS** > **Dyn.-DNS-List**

2.17.8.5 Network name

Displays the name of the network in which the host is located.

Console path:

Setup > **DNS** > **Dyn.-DNS-List**

2.17.9 DNS destinations

Requests for certain domains can be explicitly forwarded to particular remote sites.

Console path:

Setup > **DNS**

2.17.9.1 Domain name

Here you can enter the domain and assign it a dedicated remote device or a DNS server in order to resolve the name of a certain domain from another DNS server.

Console path:

Setup > **DNS** > **DNS-Destinations**

Possible values:

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

Default:

empty

2.17.9.2 Peer

Specify the remote station for DNS forwarding.

Console path:

Setup > **DNS** > **DNS-Destinations**

Possible values:

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

Default:

empty

2.17.9.3 Rtg-Tag

The routing tag makes it possible to specify multiple forwarding definitions that are independent of each other (especially general wildcard definitions with "*"). Depending on the routing context of the requesting client, the router considers only the forwarding entries that are identified accordingly and the general entries marked with "0".

Console path:

Setup > **DNS** > **DNS-Destinations**

Possible values:

0 … 65535

Default:

0

2.17.10 Service location list

Here you configure if and to which station certain services are to be resolved.

Console path:

Setup > **DNS**

2.17.10.1 Service name

Specify here which service should be resolved by DNS, and how.

The service ID is the service that is to be resolved in accordance with RFC 2782.

By way of illustration, the following example lists several entries used to resolve SIP services:

Service name	Host name	Port
_sips._tcp.myhome.intern	.	0
_sip._tcp.myhome.intern	myhost.myhome.intern	5060
_sip._udp.myhome.intern	[self]	5060

Console path:

Setup > **DNS** > **Service-Location-List**

Possible values:

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

Default:

empty

2.17.10.2 Host name

The station name indicates which station provides the indicated service. For example, if you have a computer named `myhost` and your domain name is `myhome.internal`, then you should enter the station name here as `myhost.myhome.intern`. The station name "[self]" can be specified as the name if it is the device itself. A period "." can be entered if this service is blocked and therefore should not be resolved. (In this case any definition in the following port field will be ignored).

Console path:

Setup > **DNS** > **Service-Location-List**

Possible values:

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

Default:

empty

2.17.10.3 Port

The service port denotes the port number used for the defined service at the named client.

Console path:

Setup > **DNS** > **Service-Location-List**

Possible values:

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

Default:

0

2.17.10.4 Rtg-Tag

The routing tag determines whether and how the device should resolve specific service requests within the current tag context.

Console path:

Setup > **DNS** > **Service-Location-List**

Possible values:

0 … 65535

Default:

0

2.17.11 Dynamic SRV list

The dynamic SRV list stores service location records that the device uses itself. For example, the VoIP module enters itself here.

Console path:

Setup > **DNS**

2.17.11.1 Service name

Name of the service.

Console path:

Setup > **DNS** > **Dynamic-SRV-List**

2.17.11.2 Host name

Name of the station providing this service.

Console path:

Setup > **DNS** > **Dynamic-SRV-List**

2.17.11.3 Port

Port used to register this service.

Console path:

Setup > **DNS** > **Dynamic-SRV-List**

2.17.12 Resolve domain

If this option is active, the device answers queries about its own domain with its own IP address.

Console path:

Setup > **DNS** > **Dynamic-SRV-List**

Possible values:

No
Yes

Default:

Yes

2.17.13 Sub domains

Here a separate domain can be configured for each logical network.

Console path:

Setup > **DNS**

Possible values:

No
Yes

Default:

Yes

2.17.13.1 Network name

From the list of specified IP networks, enter the IP network for which a sub domain is to be defined.

Console path:

Setup > **DNS** > **Sub-Domains**

Possible values:

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

Default:

empty

2.17.13.2 Sub domain

Sub-domain that is to be used for the selected IP network.

Console path:

Setup > **DNS** > **Sub-Domains**

Possible values:

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

Default:

empty

2.17.14 Forwarder

Using this setting you specify whether your device forwards or rejects unrecognized DNS requests.

To recognize an address, the device DNS server checks the tables in **Setup** > **DNS**

- **DNS-List**
- **Dyn.-DNS-List**
- **Service location list**
- **Dynamic SRV list**

and requests the corresponding addresses from the DHCP server, if necessary and if you allow it.

Console path:

Setup > **DNS**

Possible values:

No
Yes

Default:

Yes

2.17.15 Tag configuration

You manage the specific DNS settings for the individual tag contexts in this table. If an entry for a tag context exists, then only the DNS settings in this table apply for this context. However, if there is no entry in this table, then the global settings of the DNS server apply.

Console path:

Setup > **DNS**

2.17.15.1 Rtg-Tag

Unique interface or routing tag, its settings will override the global settings of the DNS server.

Console path:

Setup > **DNS** > **Tag-Configuration**

Possible values:

0 … 65534

Default:

0

2.17.15.2 Operating

Enables the DNS server of the device for the corresponding tag context.

Console path:

Setup > **DNS** > **Tag-Configuration**

Possible values:

No
Yes

Default:

Yes

2.17.15.3 Forwarder

Using this setting you specify whether your device forwards or rejects DNS requests that are not recognized for the specified tag context.

To recognize an address, the device DNS server checks the tables in **Setup** > **DNS**

- **DNS-List**
- **Dyn.-DNS-List**
- **Service location list**
- **Dynamic SRV list**

and requests the corresponding addresses from the DHCP server, if necessary and if you allow it.

Console path:

Setup > **DNS** > **Tag-Configuration**

Possible values:

No
Yes

Default:

Yes

2.17.15.4 DHCP usage

For the corresponding tag context, this enables or disables the resolution of station names which have requested an IP address via DHCP.

Console path:

Setup > **DNS** > **Tag-Configuration**

Possible values:

No
Yes

Default:

Yes

2.17.15.6 Resolve domain

For the corresponding tag context, this enables or disables the response of DNS requests to its own domain with the IP address of the router.

Console path:

Setup > **DNS** > **Tag-Configuration**

Possible values:

No
Yes

Default:

Yes

2.17.16 Alias-List

This menu allows you to configure alias entries for the domain name system (DNS).

Console path:

Setup > **DNS**

2.17.16.1 Alias name

Enter an alternative name for the DNS configuration here.

Console path:

Setup > **DNS** > **Alias-List**

Possible values:

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

Default:

empty

2.17.16.2 Rtg-Tag

Use this entry to define a routing tag for this alias.

Console path:

Setup > **DNS** > **Alias-List**

Possible values:

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

Default:

0

2.17.16.3 Canonical-Name

Specify here a unique CNAME for this alias.

Console path:

Setup > **DNS** > **Alias-List**

Possible values:

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

Default:

empty

2.17.17 Loopback-Addresses

This table allows you to store loopback addresses for each remote site. This means that there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one remote site and loopback address. The remote site must also be in the DNS Destinations table. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.

Console path:

Setup > **DNS**

2.17.17.1 Destination

The remote site as part of a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an @. The remote site must also be in the DNS Destinations table.

Console path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.17.17.2 Loopback address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

Console path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.17.20 Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

Console path:

Setup > **DNS**

2.17.20.1 Log DNS resolutions

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under **Setup** > **SYSLOG** > **Operating**. If you enable this option to log DNS requests, the DNS server in the device sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (`ANSWER` record or `ADDITIONAL` record) generates a SYSLOG message with the following structure `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record`.

The parameters have the following meanings:

- The `TID` (transaction ID) contains a 4-character hexadecimal code.
- The `{host name}` is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The `resource record` consists of three parts: The request, the type or class, and the IP resolution (for example `www.mydomain.com STD A resolved to 193.99.144.32`)

Console path:

Setup > **DNS** > **Syslog**

Possible values:

No

Disables the logging of DNS requests and responses.

Yes

Enables the logging of DNS requests and responses.

Default:

No

2.17.20.2 Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.

The use of the IP addresses `127.0.0.1` and `::1` to force the use of an external server is not permitted.

Console path:

Setup > **DNS** > **Syslog**

Possible values:

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

2.17.20.3 Log source

Contains the log source as displayed in the SYSLOG messages.

Console path:

Setup > **DNS** > **Syslog**

Possible values:

System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

Router

2.17.20.4 Log level

Contains the priority that is shown in the SYSLOG messages.

Console path:

Setup > **DNS** > **Syslog**

Possible values:

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Default:

Notice

2.17.20.5 Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

Console path:

Setup > **DNS** > **Syslog**

Possible values:

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

Special values:

Name of the IP networks whose address should be used
“INT” for the address of the first Intranet
“DMZ” for the address of the first DMZ
LB0 to LBF for the 16 loopback addresses
Any valid IP address

2.17.20.6 Filter name

References a SYSLOG filter.

Console path:

Setup > **DNS** > **SYSLOG**

Possible values:

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

2.17.20.7 Filter-Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the field **Filter name**, are allowed or denied.

Console path:

Setup > **DNS** > **SYSLOG**

Possible values:

Allow
Reject

Default:

Reject

2.17.20.8 Log-Server-Port

The syslog server port to use.

Console path:

Setup > **DNS** > **SYSLOG**

Possible values:

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

Default:

514

2.17.21 Tunnel-Filter

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

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

Console path:

Setup > **DNS**

2.17.21.1 Operating

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

Console path:

Setup > **DNS** > **Tunnel-Filter**

Possible values:

No

Tunnel filter is disabled.

Yes

Tunnel filter is enabled.

Default:

Yes

2.17.21.2 Minimum-TTL

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

Console path:

Setup > **DNS** > **Tunnel-Filter**

Possible values:

0 … 99

Default:

5

2.17.21.3 Address-Limit

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

Console path:

Setup > **DNS** > **Tunnel-Filter**

Possible values:

0 … 99

Default:

3

2.18 Accounting

This menu contains the configuration of the Accounting.

Console path:

Setup

Possible values:

No
Yes

Default:

Yes

2.18.1 Operating

Turn accounting on or off.

Console path:

Setup > **Accounting**

Possible values:

No
Yes

Default:

No

2.18.2 Save to flashROM

Turn accounting data in flash memory on or off. Accounting data saved to flash will not be lost even in the event of a power outage.

Console path:

Setup > **Accounting**

Possible values:

No
Yes

Default:

No

2.18.8 Time snapshot

When configuring the snapshot, the interval is set at which the accounting data are temporarily saved into a snapshot.

Console path:

Setup > **Accounting**

2.18.8.1 Index

Displays the system's internal index.

Console path:

Setup > **Accounting** > **Time-Snapshot**

2.18.8.2 Operating

Turn intermediate storage of accounting data on or off.

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

Yes
No

Default:

No

2.18.8.3 Type

Here you can set the interval at which the snapshot will be generated.

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

Daily
Weekly
Monthly

Default:

Monthly

2.18.8.4 Day

The day of the month on which caching is performed. Only relevant if the interval is "monthly".

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

0 … 31

Default:

1

2.18.8.5 Day of week

The weekday on which caching is performed. Only relevant if the interval is "weekly".

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

Unknown
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Default:

Unknown

2.18.8.6 Hour

The hour of day at which caching will be performed.

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

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

Default:

0

2.18.8.7 Minute

The minute in which caching will take place

Console path:

Setup > **Accounting** > **Time-Snapshot**

Possible values:

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

Default:

0

2.18.16 Intermittent-Reporting-Interval

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

Console path:

Setup > **Accounting**

Possible values:

0 … 30 Seconds

Special values:

0

Switched off

2.18.17 Status-Table-Entry-Limit

Specifies the maximum number of entries saved by the accounting.

Console path:

Setup > **Accounting**

Possible values:

0 … 999,999 Entries

Special values:

0

Unlimited

2.19 VPN

This menu contains the configuration of the Virtual Private Network (VPN).

Console path:

Setup

2.19.3 Isakmp

This menu contains the configuration of the Isakmp.

Console path:

Setup > **VPN**

2.19.3.4 Timer

This table contains values that affect the timing of IKE negotiations.

The values are passed to the IKE job with each full VPN configuration (setting up all VPN rules). Each time an IKE job is used it reads these values from its configuration. This means that the expiry timeout will be used immediately for every new negotiation (incl. rekeying of old connections). The retry limit is also used immediately, even during the ongoing repeats of negotiation packets.

Console path:

Setup > **VPN** > **Isakmp**

2.19.3.4.1 Retr-Lim

The retry limit specifies the maximum number of times that an IKE negotiation packet will be repeated if there is no response to it. The time interval between repeats currently cannot be configured and is 5, 7, 9, 11, 13… seconds. The overall time for IKE negotiation is also capped by the expiry limit.

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

Possible values:

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

Default:

5

2.19.3.4.2 Retr-Tim

These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations!

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

Possible values:

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

Default:

1

2.19.3.4.3 Retr-Tim-Usec

These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations!

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

Possible values:

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

Default:

0

2.19.3.4.4 Retr-Tim-Max

These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations!

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

Possible values:

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

Default:

10

2.19.3.4.5 Exp-Tim

Maximum duration of the IKE negotiation phase in seconds.

These settings are included to maintain compatibility to earlier firmware versions. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations!

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

Possible values:

0 … 65535 Seconds

Default:

30

2.19.3.4.6 Idx.

The table contains only one line, so the index only has the value "1".

Console path:

Setup > **VPN** > **Isakmp** > **Timer**

2.19.3.29 DH-Groups

This menu contains the configuration for the precalculation of DH keys.

Console path:

Setup > **VPN** > **Isakmp**

2.19.3.29.1 Precalculation

This option enables or disables the precalculation of DH keys.

Console path:

Setup > **VPN** > **Isakmp** > **DH-Groups**

Possible values:

Yes
No

Default:

Yes

2.19.3.29.2 Group-Config

This table specifies the number of DH keys to calculate for each DH group.

Console path:

Setup > **VPN** > **Isakmp** > **DH-Groups**

2.19.3.29.2.1 DH-Group

This value displays the corresponding DH group.

Console path:

Setup > **VPN** > **Isakmp** > **DH-Groups** > **Group-config**

Possible values:

Selection from the list of predefined DH groups

2.19.3.29.2.2 Precalc-Target

This value specifies the number of DH keys to be calculated for this DH group.

If you specify the value `0` here but you have enabled precalculation, the device will take the number from the policies stored in the SPD table (Security Policy Database) as a basis for calculation.

Console path:

Setup > **VPN** > **Isakmp** > **DH-Groups** > **Group-config**

Possible values:

0 … 999999999

Default:

0

2.19.4 Proposals

This menu contains the configuration of the Proposals.

Console path:

Setup > **VPN**

2.19.4.9 IKE-Proposal-Lists

Here you can display and add IKE proposal lists.

Console path:

Setup > **VPN** > **Proposals**

2.19.4.9.1 IKE-Proposal-Lists

Name for the combination of IKE proposals

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

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

Default:

empty

2.19.4.9.2 IKE-Proposal-1

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.3 IKE-Proposal-2

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.4 IKE-Proposal-3

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.5 IKE-Proposal-4

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.6 IKE-Proposal-5

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.7 IKE-Proposal-6

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.8 IKE-Proposal-7

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.9.9 IKE-Proposal-8

From the list of defined IKE proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IKE-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10 IPSEC-Proposal-Lists

Here you combine previously-defined proposals to form proposal lists.

Console path:

Setup > **VPN** > **Proposals**

2.19.4.10.1 IPSEC-Proposal-Lists

Name for the combination of IPSec proposals

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

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

Default:

empty

2.19.4.10.2 IPSEC-Proposal-1

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.3 IPSEC-Proposal-2

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.4 IPSEC-Proposal-3

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.5 IPSEC-Proposal-4

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.6 IPSEC-Proposal-5

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.7 IPSEC-Proposal-6

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.8 IPSEC-Proposal-7

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.10.9 IPSEC-Proposal-8

From the list of defined IPSec proposals, select the proposal that is to be used for this list.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC-Proposal-Lists**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.4.11 IKE

In this table you can define the proposals for administration of the SA negotiation.

Console path:

Setup > **VPN** > **Proposals**

2.19.4.11.1 Name

Name for the combinations of IKE parameters that should be used as the proposal.

The Internet Key Exchange (IKE) is a protocol for authentication and key exchange.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

2.19.4.11.2 IKE-Crypt-Alg

Encryption algorithm for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

AES-CBC
3DES-CBC
NULL-CBC

Default:

AES-CBC

2.19.4.11.3 IKE-Crypt-Keylen

Key length for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

0 … 65535

Default:

128

2.19.4.11.4 IKE-Auth-Alg

Hash algorithm for the encryption. The available values depend on the device you want to configure.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384
SHA2-512

Default:

MD5

2.19.4.11.5 IKE-Auth-Mode

Authentication method for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

Preshared key
Symmetrical PSK requires the key to be known at both ends of the connection.

RSA-Signature
Asymmetrical method with private and public keys, known from Rivest, Shamir Adleman.

Default:

Preshared key

2.19.4.11.6 Lifetime-Sec

Validity of the connections negotiated with this proposal with respect to connection duration

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

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

Default:

108000

Special values:

0
No limit on connection time

2.19.4.11.7 Lifetime-KB

Validity of the connections negotiated with this proposal with respect to transmitted data volume.

Console path:

Setup > **VPN** > **Proposals** > **IKE**

Possible values:

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

Default:

0

Special values:

0

No limit on data volume.

2.19.4.12 IPsec

You define the defaults for encryption, authentication or compression here.

Console path:

Setup > **VPN** > **Proposals**

Possible values:

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

Default:

0

Special values:

0

No limit on data volume.

2.19.4.12.1 Name

Name for the combinations of IPSec parameters that should be used as the proposal.

IPSec stands for "IP Security Protocol" and was originally the name used by a working group of the IETF, the Internet Engineering Task Force. Over the years, this group has developed a framework for a secure IP protocol that today is generally referred to as IPSec.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

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

Default:

empty

2.19.4.12.3 ESP-Crypt-Alg

Encryption algorithm for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

None
AES-CBC
3DES-CBC
NULL

Default:

AES-CBC

2.19.4.12.4 ESP-Crypt-Keylen

Key length for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

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

Default:

256

2.19.4.12.5 ESP-Auth-Alg

ESP authentication method for this proposal.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

None
HMAC-MD5
HMAC-SHA1
HMAC-SHA2-256
HMAC-SHA2-384
HMAC-SHA2-512

Default:

HMAC-SHA1

2.19.4.12.8 Lifetime-Sec

Validity of the connections negotiated with this proposal with respect to connection duration

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

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

Default:

28800

Special values:

0

No limit on connection time

2.19.4.12.9 Lifetime-KB

Validity of the connections negotiated with this proposal with respect to transmitted data volume.

Console path:

Setup > **VPN** > **Proposals** > **IPSEC**

Possible values:

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

Default:

2000000

Special values:

0

No limit on data volume.

2.19.5 Certificates and keys

This menu contains the configuration of the certificates and keys.

Console path:

Setup > **VPN**

2.19.5.3 IKE-Keys

Entered here are the shared key for preshared-key authentication and the identities for preshared-key- and RSA signature authentication.

Console path:

Setup > **VPN** > **Certificates-and-Keys**

2.19.5.3.1 Name

Name for the combination of identities and keys.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

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

Default:

empty

2.19.5.3.2 Remote identity

Remote ID that the entered key is to be valid for.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

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

Default:

empty

2.19.5.3.3 Shared sec

Key/secret that should apply to this combination.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

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

Default:

empty

2.19.5.3.4 Shared-Sec-File

[obsolete, not used: File with PSK]

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.5.3.5 Remote-ID-Type

Type of remote ID that the entered key is to be valid for.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

No-Identity
IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

No-Identity

2.19.5.3.6 Local-ID-Type

Type of local ID that the entered key is to be valid for.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

No-Identity
IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

No-Identity

2.19.5.3.7 Local identity

Local ID that the entered key is to be valid for.

Console path:

Setup > **VPN** > **Certificates-and-Keys** > **IKE-Keys**

Possible values:

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

Default:

empty

2.19.7 Layer

Here you define further parameters for individual VPN connections.

Console path:

Setup > **VPN**

2.19.7.1 Name

Name for the combination of connection parameters.

Console path:

Setup > **VPN** > **Layer**

Possible values:

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

Default:

empty

2.19.7.3 PFS-Grp

Perfect Forward Secrecy (PFS) is a security feature of encryption algorithms. The PFS group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

Console path:

Setup > **VPN** > **Layer**

Possible values:

0

No PFS

1

MODP-768

2

MODP-1024

5
MODP-1536
14
MODP-2048
15
MODP-3072
16
MODP-4096

Default:

2

2.19.7.4 IKE-Grp

The IKE group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

Console path:

Setup > **VPN** > **Layer**

Possible values:

1
MODP-768
2
MODP-1024
5
MODP-1536
14
MODP-2048
15
MODP-3072
16
MODP-4096

Default:

2

2.19.7.5 IKE-Prop-List

Select the IKE proposal list for this connection from the list of specified IKE proposal lists.

Console path:

Setup > **VPN** > **Layer**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.7.6 IPSEC-Prop-List

Select the IPSec proposal list for this connection from the list of specified IPSec proposal lists.

Console path:

Setup > **VPN** > **Layer**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.7.7 IKE key

Select the IKE key for this connection from the list of specified IKE keys.

Console path:

Setup > **VPN** > **Layer**

Possible values:

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

Default:

empty

2.19.8 Operating

Switches the VPN module on or off.

Console path:

Setup > **VPN**

Possible values:

Operating
Deactivated

Default:

Deactivated

2.19.9 VPN peers

In this table you define the VPN connections to be established by your device.

Console path:

Setup > **VPN**

2.19.9.1 Peer

Select the name of the VPN connection from the list of defined peers.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

empty

2.19.9.2 Extranet address

In LCOS versions before 9.10, this field contained the IPv4 address used by the local stations to mask their own IP address in certain scenarios.

As of LCOS version 9.10, masquerading uses the entry under **Setup** > **WAN** > **IP-List** in the field **Masq.-IP-Addr.**.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

2.19.9.4 Layer

Select the combination of connection parameters (PFS, IKE, and IPSec parameters) to be used for this connection from the list of defined connection parameters.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

empty

2.19.9.5 dynamic

Dynamic VPN is a technology which permits VPN tunnels to be connected even to remote sites that do not have a static IP address, but a dynamic one instead.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

No

Dynamic VPN is not used.

ICMP

An ICMP packet is sent to the remote site to transmit the IP address.

UDP

A UDP packet is sent to the remote site to transmit the IP address.

B channel

A connection is established to transmit IP addresses.

D channel

If possible, IP addresses are transmitted without establishing a connection.

Default:

No

2.19.9.6 SH time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

0 … 9999

Default:

0

Special values:

9999

This value causes connections to be established immediately and without a time limit.

2.19.9.7 IKE exchange

Selects the IKE exchange mode.

Main Mode exchanges significantly more unencrypted messages during the IKE handshake than the Aggressive Mode. This is why main mode is far more secure than the aggressive mode.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Main mode
Aggressive mode

Default:

Main mode

2.19.9.8 Remote-Gw

DNS name or IP address of the remote gateway which is to be used to set up the VPN connection.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

empty

2.19.9.9 Rule creation

On/off switch and type of rule creation.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Auto

Automatically created VPN rules connect the local IP networks with the IP networks entered into the routing table for the remote site.

Manual

VPN rules are only created for the remote site for IP network relationships specified "Manually" in the firewall configuration.

Off

No VPN rule is created for the remote site.

Default:

Auto

2.19.9.10 DPD-Inact-Timeout

Dead peer detection is used when VPN clients dial in to a VPN gateway or when 2 VPN gateways are connected. This is designed to ensure that a peer is logged out if there is an interruption to the VPN connection, for example when the Internet connection is interrupted briefly. If the line were not to be monitored, then the VPN gateway would continue to list the client or the other VPN gateway as logged-on. This would prevent the peer from dialing in again as, for example, the LANCOM Advanced VPN Client does not allow a simultaneous dial-in using the same serial number.

With dead-peer detection, the gateway and peer regularly exchange "keep alive" packets. If no replies are received, the gateway will log out the peer so that this ID can be registered anew once the VPN connection has been re-established. The DPD time for VPN clients is typically set to 60 seconds.

Without line monitoring, a user with the same "identity" (user name) would be prevented from dialing in because the associated user would still be in the list for the logged-in peer.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

30 … 4.294.967.294

Special values:

0

DPD deactivated

Default:

0

2.19.9.11 IKE-CFG

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the "IKE-CFG" mode is additionally added to the entries in the connection list.

When set as server, the remote site must be configured as IKE-CFG client, and thus has to request an IP address from the server. To dial in with a LANCOM Advanced VPN Client, the option "Use IKE Config Mode" has to be activated in the connection profile.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Off

If the IKE-CFG mode is switched off, no IP addresses will be assigned for the connection. Fixed IP addresses must be defined for both ends of the connection.

Client

With this setting, the device functions as the client for this VPN connection and requests an IP address from the remote site (server). The device acts in a similar manner to a VPN client.

Server

With this setting, the device functions as the server for this VPN connection. The assignment of an IP address to the client can take place in two ways:

If the remote site is entered in the routing table, the IP address defined here will be assigned to the client.

If the remote site is not entered in the routing table, an IP address which is available from the IP pool will be taken for the dial-in connections.

Default:

Off

2.19.9.12 XAUTH

Enables the use of XAUTH for the VPN remote site selected.

If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Off

No XAUTH authentication is performed for the connection to this remote site.

Client

In the XAUTH client operating mode, the device starts the initial phase of IKE negotiation (Main mode or Aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the user name and password from the PPP table entry in which the PPP remote site corresponds to the VPN remote site defined here. There must therefore be a PPP remote site of the same name for the VPN remote site. The user name defined in the PPP table normally differs from the remote site name.

Server

In the XAUTH server operating mode, the device (after successful negotiation of the initial IKE negotiation) starts authentication with a request to the XAUTH client, which then responds with its user name and password. The XAUTH server searches for the user name in the PPP table and, if a match is found, it checks the password. The user name for this entry in the PPP table is not used.

Default:

Off

2.19.9.13 SSL-Encaps.

With this option you activate IPsec-over-HTTPS technology when actively establishing a connection to this remote site.

Please note that when the IPsec-over-HTTPS option is activated, the VPN connection can only be established when the remote site also supports this technology and when the remote site is set up to receive passive VPN connections that use IPsec over HTTPS.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

No
Yes

Default:

No

2.19.9.15 Rtg-Tag

Routing tags are used on the device in order to evaluate criteria relevant to the selection of the target route in addition to the IP address. The only routes in the routing table to be used are those with a matching routing tag. The routing tag for each VPN connection can be specified here. The routing tag is used to determine the route to the remote gateway.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

0 … 65535

Default:

0

2.19.9.16 OCSP-Check

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

Please note that the check via OCSP only checks the locking status of a certificate, but it does not check the mathematical correctness of its signature, validity period, or other usage restrictions.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

No
Yes

Default:

No

2.19.9.17 IPv4-Rules

Use this entry to specify IPv4 rules for the VPN remote stations.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

empty

2.19.9.18 IPv6-Rules

Use this entry to specify IPv6 rules for the VPN remote stations.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

empty

2.19.9.20 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

DEFAULT

2.19.10 AggrMode-Proposal-List-Default

This IKE proposal list is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Select the IKE proposal list to be used for this connection from the list of specified IKE proposal lists.

Console path:

Setup > **VPN**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

IKE_RSA_SIG

2.19.11 AggrMode-IKE-Group-Default

This IKE group is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Console path:

Setup > **VPN**

Possible values:

1

MODP-768

2

MODP-1024

5

MODP-1536

14

MODP-2048

15

MODP-3072

16

MODP-4096

Default:

2

2.19.12 Additional-Gateways

This table is used to specify a list of possible gateways for each remote site.

Console path:

Setup > **VPN**

2.19.12.1 Peer

From the list of defined VPN connections, select here the name of the VPN connection that the additional gateways defined here apply to.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.2 Gateway-1

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.3 Gateway-2

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.4 Gateway-3

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.5 Gateway-4

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.6 Gateway-5

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.7 Gateway-6

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.8 Gateway-7

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.9 Gateway-8

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.10 Begin with

Here you select the first gateway that is to be used for establishing the VPN connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

Last used
Selects the entry for the connection which was successfully used most recently.

Begin with
Start with the first entry in the list.

Random
Selects a random entry from the list.

Default:

Last used

2.19.12.11 Rtg-Tag-1

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.12 Rtg-Tag-2

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.13 Rtg-Tag-3

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.14 Rtg-Tag-4

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.15 Rtg-Tag-5

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.16 Rtg-Tag-6

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.17 Rtg-Tag-7

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.18 Rtg-Tag-8

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.19 Gateway-9

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.20 Gateway-10

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.21 Gateway-11

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.22 Gateway-12

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.23 Gateway-13

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.24 Gateway-14

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.25 Gateway-15

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.26 Gateway-16

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.27 Rtg-Tag-9

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.28 Rtg-Tag-10

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.29 Rtg-Tag-11

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.30 Rtg-Tag-12

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.31 Rtg-Tag-13

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.32 Rtg-Tag-14

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.33 Rtg-Tag-15

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.34 Rtg-Tag-16

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.35 Gateway -17

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.36 Rtg-Tag-17

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.37 Gateway -18

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.38 Rtg-Tag-18

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.39 Gateway -19

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.40 Rtg-Tag-19

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.41 Gateway -20

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.42 Rtg-Tag-20

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.43 Gateway -21

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.44 Rtg-Tag-21

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.45 Gateway -22

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.46 Rtg-Tag-22

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.47 Gateway -23

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.48 Rtg-Tag-23

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.49 Gateway -24

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.50 Rtg-Tag-24

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.51 Gateway -25

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.52 Rtg-Tag-25

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.53 Gateway -26

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.54 Rtg-Tag-26

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.55 Gateway -27

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.56 Rtg-Tag-27

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.57 Gateway -28

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.58 Rtg-Tag-28

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.59 Gateway -29

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.60 Rtg-Tag-29

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.61 Gateway -30

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.62 Rtg-Tag-30

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.63 Gateway -31

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.64 Rtg-Tag-31

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.65 Gateway -32

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

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

Default:

empty

2.19.12.66 Rtg-Tag-32

Enter the routing tag for setting the route to the relevant gateway.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.12.67 Default-Prio

This is the default priority for all gateways specified here. The highest priority is 0, the lowest 65535. All gateways are grouped together, with groups of equal priority placed next to each other on one level.

The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the priority-0 layer, regardless of its configured priority. If alternative gateways specified here do not reference a gateway group, these will also be added to the group of primary gateways.

Console path:

Setup > **VPN** > **Additional-Gateways**

Possible values:

0 … 65535

Default:

0

2.19.13 MainMode-Proposal-List-Default

This IKE proposal list is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Select the IKE proposal list to be used for this connection from the list of specified IKE proposal lists.

Console path:

Setup > **VPN**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

IKE_PRESH_KEY

2.19.14 MainMode-IKE-Group-Default

This IKE group is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

Console path:

Setup > **VPN**

Possible values:

1

MODP-768

2

MODP-1024

5

MODP-1536

14

MODP-2048

15

MODP-3072

16

MODP-4096

Default:

2

2.19.16 NAT-T-Operating

Enables the use of NAT-Traversal. NAT Traversal eliminates the problems that occur when establishing a VPN connection at the end points of the VPN tunnel.

NAT-T can only be used with VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not consider the IP header of the data packets when determining the hash value for authentication. The hash value calculated by the receiver is therefore also equivalent to the hash value entered in the packets.

If the device functions as a NAT router between the VPN end points, ensure that UDP ports 500 and 4500 are enabled in the firewall when you use NAT-T! This port is activated automatically if you use the firewall assistant in LANconfig.

Console path:

Setup > **VPN**

Possible values:

Yes
Off

Default:

Off

2.19.17 Simple-Cert-RAS-Operating

Enables simplified dial-in with certificates. The simplification is that a shared configuration can be made for incoming connections, as long as the certificates of the remote peers are signed by the issuer of the root certificate in the device. In this case a configuration has to be made for each remote peer. You find the shared configuration necessary for this with the settings for default parameters. Individual remote peers can only be excluded from this function by having their certificates revoked in a CRL (Certificate Revocation List).

Console path:

Setup > **VPN**

Possible values:

Yes
Off

Default:

Off

2.19.19 QuickMode-Proposal-List-Default

From the list of specified IPSec proposal lists, select the IPSec proposal list to be used for simplified RAS with certificates.

Console path:

Setup > **VPN**

Possible values:

Max. 17 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

ESP_TN

2.19.20 QuickMode-PFS-Group-Default

This IPSec group is used for simplified dial-in with certificates.

Console path:

Setup > **VPN**

Possible values:

0

No PFS

1

MODP-768

2

MODP-1024

5

MODP-1536

14

MODP-2048

15

MODP-3072

16

MODP-4096

Default:

2

2.19.21 QuickMode-Shorthold-Time-Default

This hold time is used for simplified dial-in with certificates.

Console path:

Setup > **VPN**

Possible values:

0 … 65535

Default:

0

2.19.22 Allow-Remote-Network-Selection

If simplified dial-in with certificates is activated for the device at headquarters, then the remote routers can suggest a network to be used for the connection during the IKE negotiation in phase 2. This network is entered, for example, when setting up the VPN connection on the remote router. The device at headquarters accepts the suggested network when this option is activated. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

When configuring the dial-in remote sites, be sure to note that each remote site requests a specific network so that no network address conflicts arise.

Console path:

Setup > **VPN**

Possible values:

Yes
Off

Default:

Off

2.19.24 Max-Concurrent-Connections

This setting determines how many VPN connections the device can establish.

The maximum value is limited by the relevant license.

Console path:

Setup > **VPN**

Possible values:

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

Default:

0

Special values:

0

With a value of 0, the device may take fully advantage of the maximum number permitted by the license. Values above the license limits are ignored.

2.19.25 Flexible-ID-Comparison

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

Console path:

Setup > **VPN**

Possible values:

Yes
No

Default:

No

2.19.26 NAT-T port for rekeying

This item sets whether the IKE packets are sent to port 500 (value = "no") or the port 4500 (value = "yes") during rekeying.

Console path:

Setup > **VPN**

Possible values:

Yes
No

Default:

No

2.19.27 SSL encapsulation allowed

Activate the 'SSL encaps' option in the general VPN settings to enable passive connection establishment to a VPN device from another VPN remote device using IPsec-over-HTTPS technology (VPN device or LANCOM Advanced VPN client).

The LANCOM Advanced VPN Client supports automatic fallback to IPsec over HTTPS. With this setting, the VPN client initially attempts to establish a connection without using the additional SSL encapsulation. If the connection cannot be made, the device then tries to connect with the additional SSL encapsulation.

Console path:

Setup > **VPN**

Possible values:

Yes
No

Default:

No

2.19.30 Anti-Replay-Window-Size

Used for detecting replay attacks, this parameter defines the size of the window (i.e. number of packets) within which a VPN device considers the sequential number of the received packets to be up-to-date. The VPN device drops packets that have a sequence number older than or duplicated within this window.

Console path:

Setup > **VPN**

Possible values:

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

Default:

0

Special values:

0

A value of 0 disables replay detection.

2.19.35 Networks

In this directory, you configure the VPN network rules for IPv4 and IPv6 connections.

Console path:

Setup > **VPN**

2.19.35.1 IPv4-Rules

In this table, you configure the VPN network rules for IPv4 connections.

Console path:

Setup > **VPN** > **Networks**

2.19.35.1.1 Name

Contains the name of this rule.

Console path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

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

Default:

empty

2.19.35.1.2 Local-Networks

Contains the local networks to which this rule applies.

The following entries are valid:

- Interface names of the IP networks whose addresses are to be used. Any interface under **Setup** > **TCP-IP** > **Network-list** can be used. The network configured there is used for each interface, unless it is configured with the address "0.0.0.0" or the type "Disabled".
- Any valid IP address, e.g. "1.2.6.4".
- Prefixes in CIDR notation, or with the netmask. Examples: "1.2.5.0/24", "192.168.0.0/255.255.0.0"
- Loopback addresses known from **Setup** > **TCP-IP** > **Loopback-List**.

Specify multiple networks by separating them with a space character or comma.

Console path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.19.35.1.3 Remote-Networks

Contains the remote networks to which this rule applies.

The following entries are valid:

- Any valid IP address, e.g. "1.2.6.4".
- Prefixes in CIDR notation, or with the netmask. Examples: "1.2.5.0/24", "192.168.0.0/255.255.0.0"
- WAN peers. The networks are then the destination prefixes of all enabled static routes from **Setup** > **IP-Router** > **IP-Routing-Table**.

Specify multiple networks by separating them with a space character or comma.

Console path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.19.35.2 IPv4-Rule-Lists

In this table, you collect the VPN network rules for IPv4 connections into a rule list.

Console path:

Setup > **VPN** > **Networks**

2.19.35.2.1 Name

Contains the name of this rule list.

Console path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

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

Default:

empty

2.19.35.2.2 Rules

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

Console path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

2.19.35.3 IPv6-Rules

In this table, you configure the VPN network rules for IPv6 connections.

Console path:

Setup > **VPN** > **Networks**

2.19.35.3.1 Name

Contains the name of this rule.

Console path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

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

Default:

empty

2.19.35.3.2 Local-Networks

Contains the local networks to which this rule applies.

The following entries are valid:

- Interface names of the IP networks whose addresses are to be used. All interfaces can be used, LAN and WAN. The interface resolves to all prefixes (except the link-local prefix "fe80::/10") configured under **Setup** > **IPv6** > **Network** > **Addresses** or to those announced in a router advertisement (also from the LANCOM router).
- Any valid IP address, e.g. "2001:db8::86".
- Prefixes in CIDR notation. Example: "2001:db8:ffe::/48"
- Loopback addresses known from **Setup** > **IPv6** > **Network** > **Loopback**.
- A network group from **Setup** > **IPv6** > **Network** > **Addresses** can also be specified. This then resolves to all prefixes of this network group.

Specify multiple networks by separating them with a space character or comma.

Console path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.19.35.3.3 Remote-Networks

Contains the remote networks to which this rule applies.

The following entries are valid:

- Any valid IP address, e.g. "2001:db8::86".
- Prefixes in CIDR notation. Example: "2001:db8:ffe::/48"
- WAN peers. The networks are then the destination prefixes of all active static routes (except the link-local prefix "fe80::/10") configured under **Setup** > **IPv6** > **Router** > **Routing-Table**.

Specify multiple networks by separating them with a space character or comma.

Console path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.19.35.4 IPv6-Rule-Lists

In this table, you collect the VPN network rules for IPv6 connections into a rule list.

Console path:

Setup > **VPN** > **Networks**

2.19.35.4.1 Name

Contains the name of this rule list.

Console path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

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

Default:

empty

2.19.35.4.2 Rules

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

Console path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

2.19.36 IKEv2

In this directory you configure the IKEv2 parameters.

Console path:

Setup > **VPN**

2.19.36.1 remote sites

In this table, you configure the IKEv2 connections to VPN partners.

The console command `show vpn` shows whether the connection is successful.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.1.1 Peer

Contains the name of the connection to the remote station.

Subsequently, this name appears in the routing table.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

2.19.36.1.2 Active

Specifies whether the VPN peer is enabled.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Yes

The VPN connection is enabled.

No

The VPN connection is disabled.

Default:

Yes

2.19.36.1.3 SH time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

0

0 … 9999

Special values:

0

The device does not actively establish a connection, but waits for data packets to arrive.

9999

Keepalive: The device establishes a permanent connection.

2.19.36.1.4 Remote gateway

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.1.5 Rtg-Tag

Contains the routing tag for this VPN connection.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

0

2.19.36.1.6 Encryption

Specifies the encryption method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Encryption**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

2.19.36.1.7 Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.8 General

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **General**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

2.19.36.1.9 Lifetimes

Specifies the lifetimes of the key used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Lifetimes**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

2.19.36.1.10 IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Off
RAS services are disabled.

Client
The device works as a RAS client and dials-in to a server.

Servers
The device works as a server. RAS clients can dial-in to it.

Default:

Off

2.19.36.1.11 Rule creation

Specifies how VPN rules are created.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Auto
The device creates the VPN rules automatically.

Manual
The device uses manually created rules.

Default:

Auto

2.19.36.1.12 IPv4-Rules

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table **Setup** > **VPN** > **Networks** > **IPv4-Rule-Lists**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.13 IPv6-Rules

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table **Setup** > **VPN** > **Networks** > **IPv6-Rule-Lists**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.14 Routing

Specifies the route used for the VPN connection.

The routes for IPv4 and IPv6 connections are located in the menu **Setup** > **VPN** > **IKEv2** > **Routing**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.15 RADIUS authorization

Here you specify the RADIUS server that performs the authorization.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**.

If you do not specify a RADIUS server for authorization, the device uses the local IKEv2 configuration.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.16 RADIUS accounting

Use this entry to specify the RADIUS server that is to be used for the accounting.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

If you do not specify a RADIUS server, no accounting takes place for this VPN peer.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.17 Comment

Enter a comment about this entry.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.18 IPv4-CFG-Pool

Use this entry to specify an IPv4 address pool for the IKEv2 peer.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

empty

2.19.36.1.19 IPv6-CFG-Pool

Use this entry to specify an IPv6 address pool for the IKEv2 peer.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

2.19.36.1.21 IPv6

This entry specifies the name of the profile of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

2.19.36.1.22 Split-DNS-Profile

Name of the Split DNS profile. The split DNS profile is only active if **IKE-CFG** is set to the value **Server**.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

2.19.36.1.23 HSVPN

Here you set the name of the HSVPN profile from the table *HSVPN profiles*.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

2.19.36.1.24 CFG-Client-Profile

Here you define the name of the client profile from the *Client Profile* table. This determines whether the device in the role CFG mode client should request an address from the CFG mode server.

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

2.19.36.1.25 Auto-IP-Profile

Using the Auto-IP parameter, a VPN central site can transmit the IP address of the Dynamic Path Selection measurement destination to a VPN branch. For this purpose, the Auto-IP parameter is configured at the central site. At the branch, the measurement destination has to be set (IPv4 " 0.0.0.0" or IPv6 "::") in order for the branch to automatically take over the measurement destination from the central site.

Enter a reference to an Auto-IP profile here (see *2.19.36.16 Auto-IP-Profiles* on page 612).

Console path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

2.19.36.2 Encryption

Use this table to configure the parameters for the IKEv2 encryption.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.2.1 Name

Contains the name of this configuration.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

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

Default:

DEFAULT

2.19.36.2.2 DH-Groups

Contains the selection of Diffie-Hellman groups.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

DH32
Curve448 (as of LCOS version 10.40)
DH31
Curve25519 (as of LCOS version 10.40)
DH30
(as of LCOS version 10.12)
DH29
(as of LCOS version 10.12)
DH28
(as of LCOS version 10.12)
DH21
(as of LCOS version 10.12)
DH20
(as of LCOS version 10.12)
DH19
(as of LCOS version 10.12)
DH16
DH15
DH14
DH5
DH2

Default:

DH14

2.19.36.2.3 PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

Yes
No

Default:

Yes

2.19.36.2.4 IKE-SA-Cipher-List

Specifies which encryption algorithms are enabled.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256

Advanced Encryption Standard (AES) 256 in Galois / Counter Mode (GCM)

AES-GCM-192

Advanced Encryption Standard (AES) 192 in Galois / Counter Mode (GCM)

AES-GCM-128

Advanced Encryption Standard (AES) 128 in Galois / Counter Mode (GCM)

Chacha20-Poly1305

ChaCha20 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*, will be supported from LCOS version 10.40.

Please note that ChaCha20-Poly1305 is currently not accelerated by hardware and is therefore not recommended for VPN scenarios where high encryption performance is required.

NULL

The data packets are no longer encrypted here. This function is only required in special scenarios and is generally not recommended.

Default:

AES-CBC-256

AES-GCM-256

2.19.36.2.5 IKE-SA-Integ-Alg-List

Specifies which hash algorithms are enabled.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default:

SHA-256

2.19.36.2.6 Child-SA-Cipher-List

Specifies which encryption algorithms are enabled in the Child-SA.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256

Advanced Encryption Standard (AES) 256 in Galois / Counter Mode (GCM)

AES-GCM-192

Advanced Encryption Standard (AES) 192 in Galois / Counter Mode (GCM)

AES-GCM-128

Advanced Encryption Standard (AES) 128 in Galois / Counter Mode (GCM)

Chacha20-Poly1305

ChaCha20 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*, will be supported from LCOS version 10.40.

Please note that ChaCha20-Poly1305 is currently not accelerated by hardware and is therefore not recommended for VPN scenarios where high encryption performance is required.

Default:

AES-CBC-256

AES-GCM-256

2.19.36.2.7 Child-SA-Integ-Alg-List

Specifies which hash algorithms are enabled in the Child-SA.

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default:

SHA-256

2.19.36.3 Auth

Use this menu to configure the parameters for the IKEv2 authentication.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.3.1 Parameter

Use this table to configure the local and a corresponding remote identity for the IKEv2 authentication.

Console path:

Setup > **VPN** > **IKEv2** > **Auth**

2.19.36.3.1.1 Name

Contains the name of this entry.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

DEFAULT

2.19.36.3.1.2 Local-Auth

Sets the authentication method for the local identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature

Authentication by RSA signature.

PSK

Authentication by pre-shared key (PSK).

Digital signature

Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

2.19.36.3.1.3 Local-ID-Type

Displays the ID type of the local identity. The device interprets the entry under **Local-ID** accordingly.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

No-Identity

The ID is the local gateway address.

If this option is selected, the entry under **Local-ID** has no effect.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

2.19.36.3.1.4 Local-ID

Contains the local identity. The significance of this entry depends on the setting under **Local-ID-Type**.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.5 Local-Password

Contains the password of the local identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.6 Remote-Auth

Sets the authentication method for the remote identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per *RFC 7427*.

EAP
Authentication by the Extensible Authentication Protocol (EAP) *RFC 3748*.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-256 on the P-256 curve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-384 on the P-384 curve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) according to *RFC 4754* with SHA-512 on the P-521 curve.

Default:

PSK

2.19.36.3.1.7 Remote-ID-Type

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

No-Identity

The device accepts all connections from remote IDs.

If this option is selected, the entry under **Remote-ID** has no effect.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

2.19.36.3.1.8 Remote-ID

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.9 Remote-Password

Contains the password of the remote identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.10 Addit.-Remote-ID-List

Contains additional remote identities as specified in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.11 Local-Certificate

Contains the local VPN certificate used by the device for outbound connections.

The corresponding VPN certificates “VPN1” to “VPN9” are configured under **Setup** > **Certificates** > **SCEP-Client** > **Certificates**.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.12 Remote-Cert-ID-Check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Yes

The device checks that the remote identity exists in the certificate.

No

The device does not check that the remote identity exists in the certificate.

Default:

Yes

2.19.36.3.1.13 Local-Dig-Sig-Profile

Contains the profile name of the local digital signature profile being used.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.14 Remote-Dig-Sig-Profile

Contains the profile name of the remote digital signature profile.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

empty

2.19.36.3.1.15 OCSP-Check

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Yes
No

Default:

No

2.19.36.3.1.16 Remote-EAP-Profile

References an *EAP profile*.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

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

Default:

DEFAULT

2.19.36.3.1.17 CRL-Check

This setting enables the checking of an X.509 certificate by certificate revocation list (CRL), which checks the validity of the remote station's certificate.

You should only switch this off if you are checking by other means, e.g. with OSCP. See *2.19.36.3.1.15 OCSP-Check* on page 576.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

No
Yes

Default:

Yes

2.19.36.3.1.18 PPK-ID

Points to a *PPK*.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 66 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.3.2 Addit.-Remote-ID-List

Use this table to configure lists of additional remote identities.

Console path:

Setup > **VPN** > **IKEv2** > **Auth**

2.19.36.3.2.1 Name

Sets the name of the ID list.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Possible values:

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

Default:

empty

2.19.36.3.2.2 Addit.-Remote-IDs

Contains the remote identities that you want to collect into this list. The IDs are located in the table **Addit.-Remote-IDs**.

Specify several IDs by separating them with a space character.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Possible values:

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

Default:

empty

2.19.36.3.3 Addit.-Remote-IDs

Use this table to configure additional remote identities.

Console path:

Setup > **VPN** > **IKEv2** > **Auth**

2.19.36.3.3.1 Name

Contains the name of this remote identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

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

Default:

empty

2.19.36.3.3.2 Remote-Auth

Sets the authentication method for the remote identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

2.19.36.3.3.3 Remote-ID-Type

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

No-Identity
The device accepts all connections from remote IDs.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

2.19.36.3.3.4 Remote-ID

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

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

Default:

empty

2.19.36.3.3.5 Remote-Password

Contains the password of the remote identity.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

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

Default:

empty

2.19.36.3.3.6 Remote-Cert-ID-Check

This function checks whether the specified remote ID is also included in the certificate that was used by the peer to establish the connection.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Yes
No

Default:

Yes

2.19.36.3.3.7 OCSP-Check

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

Please note that the check via OCSP only checks the locking status of a certificate, but it does not check the mathematical correctness of its signature, validity period, or other usage restrictions.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

No
Yes

Default:

No

2.19.36.3.3.8 Remote-Dig-Sig-Profile

This entry contains the name of the remote digital signature profile.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

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

Default:

DEFAULT

2.19.36.3.3.11 PPK-ID

Points to a *PPK*.

Console path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Max. 66 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.3.4 Digital-Signature-Profiles

Use this table to configure the profiles of the digital signature.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.3.4.1 Name

Name of the profile.

Console path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

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

Default:

DEFAULT

2.19.36.3.4.2 Auth-Method

Sets the authentication method for the digital signature.

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

Console path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

RSASSA-PSS

RSASSA-PKCS1-v1_5

ECDSA

Elliptic Curve Digital Signature Algorithm

EdDSA25519

Authentication as per EdDSA25519 (Edwards Curve 2551) according to *RFC 8420*.

EdDSA448

Authentication as per EdDSA448 (Edwards Curve 448) according to *RFC 8420*.

Default:

RSASSA-PSS

2.19.36.3.4.3 Hash algorithms

Sets the hash algorithms for the digital signature.

Console path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

SHA-512, SHA-384, SHA-256, SHA1

Default:

SHA-512, SHA-384, SHA-256, SHA1

2.19.36.3.5 EAP-Profiles

This table is used to configure the EAP profiles.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.3.5.1 Name

Give this EAP profile a name that can be used to reference it.

Console path:

Setup > **VPN** > **IKEv2** > **EAP-Profiles**

Possible values:

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

2.19.36.3.5.4 EAP-Only-Authentication

Optionally allows mutual authentication of remote sites within the EAP. Authentication outside the EAP is then not required. See also *RFC 5998*

Console path:

Setup > **VPN** > **IKEv2** > **EAP-Profiles**

Possible values:

No
Yes

Optional authentication of the remote sites within the EAP.

2.19.36.3.6 PPKs

Quantum computers pose a potential challenge to current cryptographic algorithms, such as those used in IKEv2 VPN. Current algorithms are considered to be very robust, but the challenge is that an attacker can record encrypted data today and decrypt it using quantum computers in the future.

The *RFC 8784* "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security" offers a way to resist quantum computers when passwords (PSKs) are used. The extension works by "mixing" the standard IKEv2 password key (PSK) with another key in the form of a Post-quantum Preshared Key (PPK) to increase resistance.

Existing IKEv2 PSK tunnels can easily be supplemented with PPKs. The PPK is independent of the existing PSK.

LCOS supports manual configuration of PPKs. Automatic procedures for changing PPKs are not supported.

This table is used to configure the PPKs.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.3.6.1 PPK-ID

Set a unique name for this entry. The input format can be a string or hexadecimal number (identified by a leading 0x).

Console path:

Setup > **VPN** > **IKEv2** > **PPKs**

Possible values:

Max. 66 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.3.6.2 PPK

Enter the post-quantum preshared key here as a character string or hexadecimal number (identified by a leading 0x).

Console path:

Setup > **VPN** > **IKEv2** > **PPKs**

Possible values:

Max. 66 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.3.6.3 Required

If the use of PPKs is configured as required, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

Console path:

Setup > **VPN** > **IKEv2** > **PPKs**

Possible values:

No
Yes

Default:

No

2.19.36.4 General

Use this table to configure the general IKEv2 parameters.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.4.1 Name

Contains the name of this entry.

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

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

Default:

DEFAULT

2.19.36.4.2 DPD-Inact-Timeout

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

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

Default:

30

2.19.36.4.7 Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. You can set the ports 443 or 4500 instead. Use this in combination to configure any **Destination-Port**. If the setting is different

from 500, UDP encapsulation is performed automatically. The configurable port can be used for scenarios where a LANCOM router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

Incoming VPN tunnels continue to be accepted on the default ports 443, 500 and 4500. These cannot be freely configured.

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

UDP

The IKEv2 tunnel is established either with port 4500 or with the setting for the destination port. If the destination port is set to 500, this will be ignored and port 4500 is used instead.

SSL

The IKEv2 tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead.

None

The IKEv2 tunnel is established with port 500. The setting for the destination port is ignored.

Default:

None

2.19.36.4.8 Destination-Port

Here you can specify the destination port for the IKEv2 connection depending on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

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

Default:

0

2.19.36.4.9 MOBIKE

Defines whether MOBIKE as per *RFC 4555* should be supported.

MOBIKE according to RFC 4555 for IKEv2 optionally allows mobile clients to roam between different networks without disconnecting the VPN tunnel. For example, a VPN client can roam seamlessly from cellular to Wi-Fi, whereby an IKEv2 update message updates the external IP address on the VPN gateway. The advantage is that the VPN tunnel or the Security Associations (SAs) do not have to be terminated and setup again.

MOBIKE is only supported as a responder role, i.e. when VPN clients establish connections to the LANCOM VPN router. The establishment of VPN tunnels with the MOBIKE extension is not supported.

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Yes

MOBIKE is supported.

No

MOBIKE is not supported.

Default:

Yes

2.19.36.4.10 MOBIKE-Cookie-Challenge

Defines whether the device should send a cookie challenge to determine whether the VPN client can actually receive packets at the new address ("Return Routability Check").

Console path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Yes

MOBIKE-Cookie-Challenge is sent.

No

MOBIKE-Cookie-Challenge is not sent.

Default:

No

2.19.36.5 Lifetimes

Use this table to configure the lifetimes of the IKEv2 keys.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.5.1 Name

Contains the name of this entry.

Console path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

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

Default:

DEFAULT

2.19.36.5.2 IKE-SA-Sec

Contains the time in seconds until the IKE SA key is renewed.

Console path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

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

Default:

86400

Special values:

0

No key renewal.

2.19.36.5.3 IKE-SA-KB

Contains the data volume in kilobytes until the IKE SA key is renewed.

Console path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

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

Default:

0

Special values:

0

No key renewal.

2.19.36.5.4 Child-SA-Sec

Contains the time in seconds until the CHILD SA key is renewed.

Console path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

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

Default:

14400

Special values:

0

No key renewal.

2.19.36.5.5 Child-SA-KB

Contains the data volume in kilobytes until the CHILD SA key is renewed.

Console path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

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

Default:

2000000

Special values:

0

No key renewal.

2.19.36.6 Routing

Use this menu to configure the routing table for the IKEv2 routing.

The routing tables specify IPv4/IPv6 routes used by the VPN connections if there is no corresponding route in the IPv4/IPv6 router.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.6.1 IPv4

Use this table to configure the IPv4 tables for the IKEv2 routing.

Console path:

Setup > **VPN** > **IKEv2** > **Routing**

2.19.36.6.1.1 Name

Contains the name of this entry.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

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

Default:

DEFAULT

2.19.36.6.1.2 Networks

Contains the comma-separated list of IPv4 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/netmask
- IP address/netmask@tag
- IP address/prefix length
- IP address/prefix length@tag
- IP interface name
- IP interface name@tag

The specification with routing tag is used for HSVPN.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

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

2.19.36.6.1.3 Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

No

The IPv4 address is not sent

Yes

The IPv4 address will be sent

Default:

Yes

2.19.36.6.2 IPv6

Use this table to configure the IPv6 tables for the IKEv2 routing.

Console path:

Setup > **VPN** > **IKEv2** > **Routing**

2.19.36.6.2.1 Name

Contains the name of this entry.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

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

Default:

DEFAULT

2.19.36.6.2.2 Networks

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 address/prefix length@tag
- IPv6 interface name
- IPv6 interface name@tag

The specification with routing tag is used for HSVPN.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

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

2.19.36.6.2.3 Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

Console path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

No

The IPv6 address is not sent

Yes

The IPv6 address will be sent

Default:

Yes

2.19.36.7 IKE-CFG

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the IKE-CFG mode “Server” is specified for the entries in the connection list.

Use this menu to configure the address pool that the device in CFG mode “Server” passes to the clients.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.7.1 IPv4

In this table, you configure the IPv4 addresses of the address pool for the IKEv2-CFG mode “Server”.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

2.19.36.7.1.1 Name

Contains the name of the IPv4 address pool.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

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

2.19.36.7.1.2 Start-Address-Pool

Here you enter the first IPv4 address of the pool of addresses that you want to provide to dial-in clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9]./`

Default:

empty

2.19.36.7.1.3 End-Address-Pool

Here you enter the last IPv4 address of the pool of addresses that you want to provide to dial-in clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9]./`

Default:

empty

2.19.36.7.1.4 Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.19.36.7.1.5 Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

2.19.36.7.1.5 Netmask

Optional netmask sent along with the negotiated IP address.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

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

Default:

empty

2.19.36.7.2 IPv6

In this table, you configure the IPv6 addresses of the address pool for the IKEv2-CFG mode "Server".

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

2.19.36.7.2.1 Name

Contains the name of the IPv6 address pool.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

2.19.36.7.2.2 Start-Address-Pool

Here you enter the first IPv6 address of the pool of addresses that you want to provide to dial-in clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

2.19.36.7.2.3 End-Address-Pool

Here you enter the last IPv6 address of the pool of addresses that you want to provide to dial-in clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

2.19.36.7.2.4 Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

2.19.36.7.2.5 Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

2.19.36.7.2.6 PD-Source

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter "First address" to the value "::1" in the "Last address" to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- First address: 0:0:0:0001::1
- Last address: 0:0:0:0001::9

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

Default:

empty

2.19.36.7.2.7 Prefix-Length

Optional prefix length sent for the negotiated IP address.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

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

Default:

128

2.19.36.7.3 Split-DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. "*.company.com") to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

Split DNS for IKEv2 is supported by LANCOM VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

2.19.36.7.3.1 Domain-Lists

Here you specify the domain lists for split DNS.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

2.19.36.7.3.1.1 Domain-name

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. "company.internal". Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

Possible values:

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

Default:

empty

2.19.36.7.3.1.3 Domain-List

Enter a name for the domain lists.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

Possible values:

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

Default:

empty

2.19.36.7.3.4 Profiles

Here you set the profiles for split DNS.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

2.19.36.7.3.4.1 Name

Enter a name for this profile.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

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

Default:

empty

2.19.36.7.3.4.2 Send-DNS-Forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

No
Yes

Default:

No

2.19.36.7.3.4.3 Send-local-Domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

No
Yes

Default:

No

2.19.36.7.3.4.4 Domain-List

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

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

Default:

empty

2.19.36.7.4 Client-Profile

In this table you can specify whether the device in the role CFG-Mode client should request an address from the CFG-Mode server. This function is usually used in conjunction with IKEv2 routing.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

2.19.36.7.4.1 Name

Here you set a name for the Client profile.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profile**

Possible values:

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

2.19.36.7.4.2 Request-Address

Defines which address type should be requested in Config mode.

Console path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Client-Profile**

Possible values:

None
IPv4
IPv6

Default:

IPv4

IPv6

2.19.36.8 MTU

This entry contains the maximum transmission unit (MTU) for IKEv2.

Console path:

Setup > **VPN** > **IKEv2**

Possible values:

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

0 … 65535

Default:

0

Special values:

0

The MTU setting is disabled. The two IKEv2 endpoints negotiate the MTU between themselves.

2.19.36.9 RADIUS

This menu contains the RADIUS configuration for IKEv2.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.9.1 Authorization

This menu contains the configuration for the RADIUS authorization via IKEv2.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS**

2.19.36.9.1.1 Servers

This table contains the server configuration for the RADIUS authorization under IKEv2.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

2.19.36.9.1.1.1 Name

Specify an identifier for this entry.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.2 Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.3 Port

Specify the UDP port of the RADIUS server.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

1812

2.19.36.9.1.1.4 Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.6 Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.19.36.9.1.1.7 Loopback address

This entry contains the loopback address of the LANCOM gateway that sent the request to the RADIUS server.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.8 Attribute-Values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.9 Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.1.1.10 CoA active

Here you enable/disable **CoA**.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Activated
Not activated

Default:

Not activated

2.19.36.9.1.1.11 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

2.19.36.9.1.2 Password

Here you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the LANCOM gateway after this receives the corresponding authorization in the `access-accept` message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

Possible values:

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

Default:

empty

2.19.36.9.2 Accounting

This menu contains the configuration for the RADIUS accounting via IKEv2.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS**

2.19.36.9.2.1 Server

This table contains the server configuration for the RADIUS accounting under IKEv2.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

2.19.36.9.2.1.1 Name

Specify an identifier for this entry.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.1.2 Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.1.3 Port

Specify the UDP port of the RADIUS server.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

1813

2.19.36.9.2.1.4 Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.1.5 Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.19.36.9.2.1.6 Loopback address

This entry contains the loopback address of the LANCOM gateway that sent the request to the RADIUS server.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.1.7 Attribute-Values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.1.8 Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

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

Default:

empty

2.19.36.9.2.2 Interim-Interval

Set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of ±10% to keep the update messages of parallel accounting sessions separate from one another.

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

Possible values:

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

0 … 4294967295

Default:

0

Special values:

0

The transmission of interim-update messages is disabled.

2.19.36.10 Create-Routes-For-RAS-SAs

Specifies whether routes should be generated automatically from the VPN rules for dial-in (RAS) clients operating as CFG-mode servers. Disabling automatic route generation is useful when the routes are to be created by means of a routing protocol.

Console path:

Setup > **VPN** > **IKEv2**

Possible values:

No

No routes are generated for RAS SAs.

Yes

Routes are generated for RAS SAs.

Default:

Yes

2.19.36.11 Extended parameters

This table contains extended parameters for IKEv2 remote stations.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.11.1 Name

Name of the remote device.

Console path:

Setup > **VPN** > **IKEv2** > **Extended-Parameters**

Possible values:

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

Default:

empty

2.19.36.11.2 PRF-as-Sig-Hash

Specifies whether to use the PRF (pseudo-random function) of the IKEv2 negotiation as a signature hash with the RSA signature. This function should be used for compatibility with third-party products only. The setting must be configured identically at both ends of the VPN connection.

Console path:

Setup > **VPN** > **IKEv2** > **Extended-Parameters**

Possible values:

Yes
No

Default:

No

2.19.36.12 Cookie-Challenge

IKEv2 offers cookie notification, a challenge-response procedure that the IKEv2 responder can trigger if it has too many half-open IKEv2 connections. This makes the responder more resistant to DDoS attacks.

Cookie notification has been implemented to improve the compatibility with third-party VPN-enabled devices. It must be enabled on both VPN participants in order for a VPN connection to be established.

The IKEv2 cookie notification prevents the establishment of excessive numbers of half-open VPN connections and the attack on VPN-gateway resources (DDOS) that they cause. With cookie notification enabled, the responder only reacts to incoming VPN connections if the remote site is verified as reachable.

Enabling the IKEv2 cookie challenge adds two additional IKE messages to the VPN connection setup.

The switch activates the Cookie Challenge on the responder or gateway side.

On the initiator side, the cookie challenge is done automatically if the other side requests it. The switch has no effect on the initiator side or on the client side.

Please note that both initiator and responder must support the cookie challenge feature. If the remote site does not support cookie challenge, the VPN tunnel cannot be established. LANCOM VPN routers at both ends must have at least LCOS 10.30.

Console path:

Setup > **VPN** > **IKEv2**

Possible values:

Off
Always

Default:

Off

2.19.36.13 Tunnel-Groups

Some VPN scenarios require that a given group of VPN tunnels of a device terminates on, or establishes to, a common VPN gateway. This is necessary, for example, where VPN tunnels are configured on a cluster of load balancers and VPN tunnels use the alternative gateway list and maybe even different paths or outbound Internet connections (DSL, LTE, Ethernet) to reach the destination.

A VPN load balancer requires that the various VPN tunnels always terminate on a common VPN gateway.

IKEv2 tunnel groups is a feature that ensures that all VPN tunnels in a group always terminate on a common VPN gateway. The first VPN tunnel to be established in a group determines the common VPN gateway, and the VPN remote gateways for all of the other members of the tunnel group are transferred to this destination. Usually, this is the VPN tunnel that is established the fastest. The selection of a gateway is only performed again if all tunnel group members are unable to reach the gateway.

The function of the IKEv2 tunnel groups can basically be used independently of a load balancer.

Tunnel groups are not supported in conjunction with IKEv2 Redirect and the IKEv2 Redirect Load Balancer.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.13.1 Group-Name

Unique name for the tunnel group.

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

2.19.36.13.2 Peer-1

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

2.19.36.13.3 Peer-2

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

2.19.36.13.4 Peer-3

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

2.19.36.13.5 Peer-4

The name of a remote site of the IKEv2 VPN tunnel that terminates in the tunnel group.

Console path:

Setup > **VPN** > **IKEv2** > **Tunnel-Groups**

Possible values:

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

2.19.36.14 Enforce-Pre-Shared-Key-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for Pre-Shared Keys (PSK) with IKEv2:

- The length of the password must be at least 32 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

These rules do not apply to PSK managed and obtained by a RADIUS server.

Console path:

Setup > **VPN** > **IKEv2**

Possible values:

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

No

2.19.36.15 HSVPN-Profiles

This table is used to configure the HSVPN profiles.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.15.1 Name

Here you set a name for the HSVPN profile.

Console path:

Setup > **VPN** > **IKEv2** > **HSVPN-Profiles**

Possible values:

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

2.19.36.15.2 Rtg-Tag-List

Here you define the routing tags as a comma separated list (e.g. 1,2,3) that are to be transmitted via HSVPN. The Rtg-Tag list must be identical on both VPN partners in order for all of the desired ARF networks to be transported.

Console path:

Setup > **VPN** > **IKEv2** > **HSVPN-Profiles**

Possible values:

Max. 100 characters from `[0-9] ,`

2.19.36.16 Auto-IP-Profiles

This table is used to configure the Auto-IP profiles.

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.16.1 Name

Here you set a name for the Auto-IP profile. This is referenced under *2.19.36.1.25 Auto-IP-Profile* on page 567.

Console path:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profiles**

Possible values:

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

2.19.36.16.2 IPv4-Interface

IPv4 network used to send the IPv4 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv4 networks

Console path:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profiles**

Possible values:

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

2.19.36.16.3 IPv6-Interface

IPv6 network used to send the IPv6 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv6-LAN-Interfaces

Console path:

Setup > **VPN** > **IKEv2** > **Auto-IP-Profiles**

Possible values:

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

2.19.36.34 Auto-IP-Profiles

Defines the IPv6 prefix with which no VPN connections should be established. If, for example, an upstream router only assigns a Unique Local Address (ULA) from the prefix “fc00::/7” to the device, it can be prevented that the device establishes a VPN connection to a global IPv6 address with a send address from this prefix. This can be combined with the alternative gateway list where an IPv4 address is listed as an alternative gateway and then used.

Input value: IPv6 prefix, for example “fc00::/7”.

Console path:

Setup > **VPN** > **IKEv2**

Possible values:

Max. 253 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.35 Mesh

This item is used for the settings for the LANCOM Advanced Mesh VPN (AMVPN).

Console path:

Setup > **VPN** > **IKEv2**

2.19.36.35.1 Operation-Mode

This parameter affects the way the Mesh VPNs works and enables behavior as a spoke or hub, or even both roles at the same time.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

Inactive
Spoke
Hub

Default:

Inactive

2.19.36.35.2 Admin-Distance

The distance set in the IP router for routes received via the mesh tunnel.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

0 … 255

Special values:

0

Equivalent to the internal default of “15”

Default:

0

2.19.36.35.3 VPN-Peer-Template

This parameter refers to an entry in the IKEv2 peer table. This entry is used as a configuration template for the Mesh VPN tunnels.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

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

Default:

empty

2.19.36.35.4 Initial-Rate-Limit-Sec

Requested networks (addresses) are temporarily blocked in order to protect the network. The initial lockout period is specified here in seconds.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

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

Default:

5

2.19.36.35.5 Max-Rate-Limit-Sec

The blocking time from *2.19.36.35.4 Initial-Rate-Limit-Sec* on page 615 is doubled until the value set here is reached.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

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

Default:

320

2.19.36.35.6 Request-Validity-Sec

After the lockout period has expired, networks (addresses) that were previously requested will still be available. This validity always begins when the blocking expires and ends when the device sends or receives a request for this network (this address).

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

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

Default:

3600

2.19.36.35.7 Group-ID

Each device can be assigned to a group that is used to send its requests. One option of this is to divide the mesh into smaller groups, e.g. regional mesh structures.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

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

Default:

1

2.19.36.35.8 Accepted-Group-IDs

A comma-separated list specifying the mesh group IDs that are accepted. A request from a group ID not listed here will be discarded.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

Max. 253 characters from `[0-9],`

Default:

1

2.19.36.35.9 Detect-on-VPN-Peers

A comma-separated list of VPN peers that the (firewall) detector should react to. This entry is required for branches to detect incoming sessions. This can be left empty, e.g. for branches behind a NAT (without port forwarding) and therefore unable to act as responders for a mesh tunnel.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

Possible values:

Max. 253 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.19.36.35.10 Forwarding-Filter

This filter list can be used to filter requests to specific networks on the hub. If the requested network from a request via manufacturer-specific IKEv2 message does not match any table row, the request is allowed through (allow-all).

Console path:

Setup > **VPN** > **IKEv2** > **Mesh**

2.19.36.35.10.1 IP-Address-Prefix

Defines the prefix for which a rule should apply, e.g. 10.0.0.0/24 or 2001:db8::/32.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

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

2.19.36.35.10.2 Rtg-tag

Defines the routing tag or routing context associated with the filter rule.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

0 … 65535

Default:

0

2.19.36.35.10.3 Filter-Action

Defines the action for this filter entry.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

Allowed
Forbidden

2.19.36.35.10.4 Comment

Enter a descriptive comment here.

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.19.50 IKEv2 load balancer

Configures the IKEv2 load balancer.

Console path:

Setup > **VPN**

2.19.50.1 Operating

Activates/deactivates the IKEv2 load balancer.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer**

Possible values:

Yes
Activates the IKEv2 load balancer.

No
Deactivates the IKEv2 load balancer.

Default:

No

2.19.50.2 Instances

Load balancer instances are configured in the **Instances** table.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer**

2.19.50.2.1 VRRP-ID

VRRP-ID (router ID) to be used for this IKEv2 load balancer instance. VRRP must be activated on this device and configured for this VRRP ID.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

0 … 255

Default:

1

2.19.50.2.2 Local IPv4 redirect target

IPv4 address or FQDN on which the device is to receive VPN tunnels. A VPN client is forwarded to this address by the master in the load-balancer cluster.

This is not the virtual VRRP-IP address.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

2.19.50.2.3 Local-IPv6-Redirect-Target

Global IPv6 address or FQDN where the device should accept VPN tunnels. A VPN client will be redirected to this address by the master in the load balancer group. Link-local addresses are not supported.

This is not the virtual VRRP IP address.

Console path:

Setup > **VPN** > **Load-Balancer** > **Instances**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9].-:%?`

2.19.50.2.4 Message-Profile

Message profile to be used for this instance. The message profile contains the parameters for the status protocol, which the device uses to communicate its status information to the load balancer group.

If an IPv6 address is configured here, the IPv6 firewall rule ALLOW_VLB must also be enabled.

Console path:

Setup > **VPN** > **Load-Balancer** > **Instances**

Possible values:

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

Default:

DEFAULT

2.19.50.2.5 Redirection mode

Specifies at which phase of the IKEv2 negotiation the VPN gateway redirects clients to another gateway.

This parameter only takes effect if the device is VRRP master.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

IKEv2-Init

The redirect message is sent in the IKE_SA_INIT response from the VPN gateway.

IKEv2-Auth

The redirect message is sent in the IKE_AUTH phase after the client has identified itself to the VPN gateway.

Default:

IKEv2-Init

2.19.50.2.6 Redirection destinations

Specifies the destination to which the VPN client is redirected.

The parameter only takes effect if the device is VRRP master.

This can be used to configure scenarios in which the load balancer master only distributes the clients, but does not terminate any VPN tunnels itself.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

Local or remote

Clients are redirected to the device's own IP address and also to other remote gateways in the cluster.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed between all gateways except for the master gateway.

2.19.50.2.7 Comment

Contains a comment about this instance.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

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

2.19.50.2.8 VLB-Interface

Defines the interface or logical network where the IKEv2 load balancer should accept VPN tunnels. VRRP must also be configured or active on this interface.

Console path:

Setup > **VPN** > **Load-Balancer** > **Instances**

Possible values:

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

2.19.50.2.9 VLB-ID

Defines the unique identifier of the load balancer instance.

Console path:

Setup > **VPN** > **Load-Balancer** > **Instances**

Possible values:

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

Default:

1

2.19.50.3 Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer**

2.19.50.3.1 Name

Unique name for this profile

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

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

2.19.50.3.2 Interface

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

Entries from the IPv4 networks table

2.19.50.3.3 IP address

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

IPv4 address `[0-9.]`

Default:

239.255.22.11

2.19.50.3.4 Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

1987

2.19.50.3.5 Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

500

2.19.50.3.6 Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.

The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

3000

2.19.50.3.7 Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 9

Default:

5

Special values:

0

Disables the replay detection.

2.19.50.3.8 Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 255

Default:

15

2.19.50.3.9 Key

Shared secret for the load balancer communication log.

The secret must be the same on all of the VPN gateways in a cluster.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

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

2.19.50.3.10 Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

None
AES-128-GCM
AES-192-GCM
AES-256-GCM

Default:

None

2.19.50.3.11 HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

None
96 bits
128 bits

Default:

96 bits

2.19.50.3.12 Comment

Contains a comment about this message profile.

Console path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

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

2.19.64 OCSP-Client

This menu contains the settings for the OCSP client.

Console path:

Setup > **VPN**

2.19.64.1 OCSP-Client active

This setting activates the OSCP client.

SNMP ID: 2.19.64.1

Telnet path: /Setup/VPN

Possible values:

- No
- Yes

Default: No

2.19.65 Gateway-Groups

This table contains the settings for gateway groups, which you can reference in the list of additional gateways (see *2.19.12 Additional-Gateways* on page 531).

Console path:

Setup > **VPN**

2.19.65.1 Group-Name

Give this gateway group a unique name so that you can reference the group later.

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.19.65.2 Priority

The priority of this group.

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

0 … 65535

2.19.65.3 Begin-With

Selection strategy within the group.

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

Last-Used

Selects the gateway in the group which successfully connected most recently.

First

Start with the first entry in the list.

Random

Selects a random entry from the list.

2.19.65.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **VPN** > **Gateway-Groups**

Possible values:

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

2.19.66 Gateway-Mappings

This table contains the settings for gateway mapping. Gateway mappings allow you to set up gateway groups (see also *2.19.65 Gateway-Groups* on page 625), which you can reference under *2.19.12 Additional-Gateways* on page 531. The gateway and group name together form the primary key of the table, i.e. the combination of the two must be unique in the table. This allows a single gateway to be mapped to multiple groups, if desired.

Console path:

Setup > **VPN**

2.19.66.1 Group-Name

Name of the group that the gateway belongs to.

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.19.66.2 Gateway

DNS name or IP address of a gateway.

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

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

2.19.66.3 Rtg-Tag

Routing tag of the gateway.

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

0 … 65535

Default:

0

2.19.66.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **VPN** > **Gateway-Mappings**

Possible values:

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

2.19.67 Negotiation control

With the negotiation control, you set the number of VPN negotiations allowed at the same time. In the "Normal" setting, this is 7 simultaneous negotiations. In the "Medium" setting, 21 simultaneous negotiations are possible and with "Fast" 49 simultaneous negotiations are possible.

Pfad Konsole:

Setup > **VPN**

Mögliche Werte:

Normal
Medium
Fast

Default-Wert:

Normal

2.20 LAN-Bridge

This menu contains the settings for the LAN bridge.

Console path:

Setup

Possible values:

No
Yes

Default:

No

2.20.1 Protocol version

Select the desired protocol here. Depending on the choice made here, the device uses either the classic protocol or the rapid protocol, as defined in the IEEE 802.1D-1998, chapter 8 and IEEE 802.1D-2004 chapter 17 respectively.

Console path:

Setup > **LAN-Bridge**

Possible values:

Classic
Rapid

Default:

Classic

2.20.2 Bridge priority

This value sets the priority of the bridge in the LAN. This value influences which bridge the spanning tree protocol takes to be the root bridge. This is a 16-bit value (0 .. 65535), where higher values mean lower priority. You should only change the default value if you prefer a certain bridge. The selection process still works even if all the values are the same because, if the priorities are identical, the device uses the MAC address of the bridge to make the decision.

Even though an entire 16-bit parameter is available for configuring this parameter, special care should be taken where newer versions of the rapid or multiple spanning tree protocol are involved. The priority value should only be changed in increments of 4096, because the lower 12 bits are used for other purposes. This could mean that these values may be ignored by future firmware releases.

Console path:

Setup > **LAN-Bridge**

Possible values:

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

Default:

32768

2.20.4 Encapsulation table

This table is used to add the encapsulation methods.

Console path:

Setup > **LAN-Bridge**

2.20.4.1 Protocol

A protocol is identified by its 16-bit protocol identifier carried in the Ethernet II/SNAP type field (often referred to as the Ethertype). The protocol type is written as a hexadecimal number from `0001` to `ffff`. Even if the table is empty, some protocols are implicitly assumed to be listed in this table as type SNAP (such as IPX and AppleTalk). This can be overridden by explicitly setting their protocol to Ethernet II.

Console path:

Setup > **LAN-Bridge** > **Encapsulation-Table**

2.20.4.2 Encapsulation

Here you can specify whether or not data packets are to be given an Ethernet header when being transmitted. Normally you should enter the option "Transparent". The "Ethernet" option should only be chosen if you wish to combine a layer for use with the bridge.

Console path:

Setup > **LAN-Bridge** > **Encapsulation-Table**

Possible values:

Transparent
Ethernet

Default:

Transparent

2.20.5 Max-Age

This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as "aged". This defines how quickly the spanning-tree algorithm reacts to changes, for example due to failed bridges. This is a 16-bit value (0 .. 65535).

Console path:

Setup > **LAN-Bridge**

Possible values:

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

Default:

20

2.20.6 Hello-Time

This parameter specifies the time interval in seconds in which the device operating as the root bridge sends information to the LAN.

Console path:

Setup > **LAN-Bridge**

Possible values:

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

Default:

2

2.20.7 Forward delay

This value determines the time (in seconds) that passes before a port should change from "listening" to "learning" or from "learning" to "forwarding". However, now that rapid spanning tree offers a method of determining when a port can be switched into the "forwarding state" without a long wait, this setting in many cases no longer has any effect.

Console path:

Setup > **LAN-Bridge**

Possible values:

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

Default:

6

2.20.8 Isolated mode

This item allows connections to be switched on or off, such as those between layer-2 forwarding and the LAN interfaces.

Please note that other functions relating to the connection (e.g. spanning tree, packet filters) continue to function, independent of whether the interfaces are switched on or off.

Console path:

Setup > **LAN-Bridge**

Possible values:

Bridge
Router (isolated mode)

Default:

Bridge

2.20.10 Protocol table

You can add the protocols to be used over the LAN bridge here.

Console path:

Setup > **LAN-Bridge**

2.20.10.1 Name

This name should describe the rule. Note that this is also the content column (index column) of the table, i.e. the content of the table is a string.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Max. 15 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.20.10.2 Protocol

The identifier of the protocol is entered here. The identifier is a 4-digit hexadecimal number that uniquely identifies each protocol. Common protocols include 0800, 0806 for IP and ARP (Internet), E0E0, 8137 for IPX (Novell Netware), F0F0 for NetBEUI (Windows networks), or 809B, 80F3 for AppleTalk (Apple networks). If you set the protocol field to zero, this rule affects all packets. Other protocols are referred to in the documentation.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

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

Default:

empty

2.20.10.3 Sub-protocol

Enter the sub-protocol here. Common sub-protocols within the IP protocol (0800) include 1 ICMP, 6 TCP, 17 UDP, 50 ESP (IPsec). This field specifies the ARP frame type (ARP request/reply, RARP request/reply) for ARP packets. If this value is unequal to 0, the rule will only match if either the packet is an IPv4 packet and the IP protocol (UDP, TCP, ICMP,…) matches the given value, or if it is an ARP packet and the ARP type matches the given value. If the protocol field is set, but the sub-protocol field is set to 0, then the rule applies to all packets of the specified protocol (e.g. for all IP packets for protocol 0800).

Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

0 … 65535

Default:

0

2.20.10.4 Port

This specifies the range of port numbers for the TCP or UDP protocols. For example, UDP port 500 corresponds to the IKE used by IPsec.

If this value is not equal to 0, then the rule only applies when an IPv4 TCP or UDP packet arrives or when the source of the target TCP/UDP port is within the range defined by these two values.

If a zero (0) is entered as the end port, the rule applies only for the start port. The port numbers of the receiving port and the target port are compared, and a rule applies if just one of these is within the defined range. If the protocol and the sub-protocol are set, but the port fields have the value 0, then the rule applies to all packets of the specified sub-protocol (e.g. for all packets for protocol 0800/6).

Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

0 … 65535

Default:

0

2.20.10.5 Port-End

This specifies the range of port numbers for the TCP or UDP protocols. For example, UDP port 500 corresponds to the IKE used by IPsec.

If this value is not equal to 0, then the rule only applies when an IPv4 TCP or UDP packet arrives or when the source of the target TCP/UDP port is within the range defined by these two values.

If '0' is entered as the end port, the rule applies only for the start port. The port numbers of the receiving port and the target port are compared, and a rule applies if just one of these is within the defined range. If the protocol and the sub-protocol are set, but the port fields have the value 0, then the rule applies to all packets of the specified sub-protocol (e.g. for all packets for protocol 0800/6).

Note: Further information is to be found at www.iana.org under the section "Protocol Number Assignment Services", documents "Protocol Numbers" and "Port Numbers".

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

0 … 65535

Default:

0

2.20.10.6 Ifc list

This list contains the LAN interfaces for which the rule applies. The syntax of the interface list is specified the in addenda/supplements/attachments.

The following pre-defined interface descriptors are used to specify the relevant interfaces in a comma-separated expression:

- LAN-1,
- WLAN-1, WLAN-1-2, WLAN-1-3, WLAN-1-4, WLAN-1-5, WLAN-1-6, WLAN-1-7, WLAN-1-8, WLAN-2, WLAN-2-2, WLAN-2-3, WLAN-2-4, WLAN-2-5, WLAN-2-6, WLAN-2-7, WLAN-2-8,
- P2P-n-m ("n" refers to the interface of the wireless LAN network and "m" is the number of the P2P connection on this WLAN).

Numerically consecutive interface identifiers can be described by the abbreviations `P2P-4~P2P-10`: If no interface is specified here, the selected action will never be executed.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

All LAN interfaces
DMZ interfaces
Logical WLAN networks and the point-to-point bridges in the WLAN

2.20.10.7 Action

This field defines the action to be taken on a packet if it matches the rule. A packet may be dropped, passed unchanged, or redirected to a different IP address. For redirection, the IP address that the packet is to be redirected to must be specified in the following field. The redirect feature is only available for packets that support TCP, UDP, or ICMP echo requests. The device will modify the destination MAC and IP address fields before forwarding the packet, and will put an entry in the Connection Table to allow back translation of possible answers.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Transmit
Discard
Redirect

Default:

Discard

2.20.10.8 Redirect IP address

If the rule is a redirect rule, this field must be used to specify which IP address the appropriate packets are to be redirected to.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.20.10.9 Dest-MAC-Addr.

The physical address (MAC) of a destination station in the wireless LAN is entered here. Every network card has its own MAC address that is unique in the world. The address is a 12-character hexadecimal number (e.g. 00A057010203). This address can generally be found printed on the network card. If you enter no MAC address (or zero), this rule affects all packets.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Max. 15 characters from `[A-F][0-9]`

Default:

empty

2.20.10.10 IP network

If the first field is set to a value unequal to `0.0.0.0`, a packet will match this rule only if it is an IPv4 packet and either the packet's source or destination address are contained in the IP network defined by these two values.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.20.10.11 IP-Netmask

If the first field is set to a value unequal to `0.0.0.0`, a packet will match this rule only if it is an IPv4 packet and either the packet's source or destination address are contained in the IP network defined by these two values.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.20.10.12 DHCP-Src-MAC

Setting this option to "Yes" or "No" activates the DHCP tracking. This checks whether the table **Status** > **LAN-Bridge** > **DHCP-Table** contains the source MAC address of a packet from a network user who obtained an IP address via DHCP. Additionally, a network can be specified for a filter rule. However, if a rule has set this parameter to "Yes", a specified network will be ignored.

If DHCP address tracking is enabled, any IP addresses entered are disregarded.

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Irrelevant

The source MAC address is not considered.

Yes

The rule applies if the source MAC address of the packet is listed in the table under **Status** > **LAN-Bridge** > **DHCP-Table** as an address that obtained an IP address via DHCP.

No

The rule applies if this is not the case.

Default:

Irrelevant

2.20.10.14 IP-Match

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

Console path:

Setup > **LAN-Bridge** > **Protocol-Table**

Possible values:

Either
Both the source and the destination address are checked.
Source
Only the source address is checked.
Destination
Only the destination address is checked.

Default:

Either

2.20.11 Port data

This table can be used to set further bridge parameters for each port.

Console path:
Setup > **LAN-Bridge**

2.20.11.2 Port

From the list of logical interfaces on the device (e.g. LAN-1, WLAN11 or P2P-1-1), select the port for which the spanning-tree parameters are to be set.

Console path:
Setup > **LAN-Bridge** > **Port-Data**

2.20.11.3 Active

This can be used to block a port completely, i.e. the port will always have the 'disabled' status.

Console path:
Setup > **LAN-Bridge** > **Port-Data**

Possible values:

No
Yes

Default:

Yes

2.20.11.5 Bridge group

Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the device to be a single interface. This can then be used for Advanced Routing and Forwarding, for example.

A requirement for data transfer from/to a logical interface via the LAN bridge is the deactivation of the global "isolated mode" which applies to the whole of the LAN bridge. Furthermore, the logical interface must be assigned to a bridge group. With the setting "none", no transfers can be made via the LAN bridge.

Console path:

Setup > **LAN-Bridge** > **Port-Data**

Possible values:

BRG-1
BRG-2
BRG-3
BRG-4
BRG-5
BRG-6
BRG-7
BRG-8
None

Special values:

If the interface is removed from all bridge groups by setting "none", then there is no communication between the LAN and WLAN via the LAN bridge (isolated mode). With this setting, LAN/WLAN data transfers over this interface are only possible via the router.

Default:

BRG-1

2.20.11.6 DHCP limit

Number of clients which can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filer table to limit access to just one logical interface.

Console path:

Setup > **LAN-Bridge** > **Port-Data**

Possible values:

0 … 255

Default:

0

2.20.11.7 Point-to-point port

This item corresponds to the "adminPointToPointMAC" setting as defined in IEEE 802.1D. By default, the "point-to-point" setting for the LAN interface is derived from the technology and the concurrent status:

An Ethernet port is assumed to be a P2P port if it is operating in full-duplex mode.

A token ring port is assumed to be a P2P port if it is operating in full-duplex mode.

A WLAN SSID is never considered to be a P2P port.

A WLAN P2P connection is always assumed to be a P2P port.

However, this automatic setting can be revised if this is unsuitable for the required configuration. Interfaces in "point-to-point" mode have various specialized capabilities, such as the accelerated port status change for working with the rapid spanning tree protocol.

Console path:

Setup > **LAN-Bridge** > **Port-Data**

Possible values:

Auto
Force true
Force false

Default:

Auto

2.20.11.9 Private mode

You have the option to enable or disable the private mode for each individual interface.

Console path:

Setup > **LAN-Bridge** > **Port-Data**

Possible values:

No
The private mode is disabled.

Yes
The private mode is enabled.

Default:

No

2.20.12 Aging time

When a client requests an IP address from a DHCP server, it can also ask for a lease period (in minutes) for the address. This values governs the maximum length of lease that the client may request. When a client requests an address without asking for a specific lease period, the value set here will apply.

Console path:

Setup > **LAN-Bridge**

Possible values:

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

Default:

300

2.20.13 Priority mapping

This table assigns a user priority to each IP packet due to be sent, based on a ToS/DSCP value as per 802.1D. An example of how user priority can be used concerns wireless LANs with activated QoS, where the packets are allocated to access categories (voice/video/best-effort/background).

Console path:

Setup > **LAN-Bridge**

2.20.13 Name

Enter a name for a combination of DSCP value and priority.

Console path:

Setup > **LAN-Bridge** > **Priority-Mapping**

Possible values:

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

Default:

empty

2.20.13.2 DSCP value

Enter the DSCP value that is used for this priority assignment.

Console path:

Setup > **LAN-Bridge** > **Priority-Mapping**

Possible values:

0 … 255

Default:

0

2.20.13.3 Priority

Enter the priority that is used for this priority assignment.

Console path:

Setup > **LAN-Bridge** > **Priority-Mapping**

Possible values:

Best-Effort
Background
Excellent-Effort
Controlled latency
Video
Voice
Network-Control

Default:

Best-Effort

2.20.20 Spanning tree

This menu contains the settings for the spanning tree.

Console path:

Setup > **LAN-Bridge**

2.20.20.1 Operating

Here you can switch the Spanning-Tree support on and off. When Spanning Tree is turned off, the router does not send any Spanning Tree packets and passes received packets along instead of processing them itself.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

No
Yes

Default:

No

2.20.20.2 Bridge priority

This value sets the priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the spanning tree protocol. This is a 16-bit value (0 .. 65535), where higher values mean lower priority. The

default value should only be changed if a certain bridge is to be preferred. The selection process still works even if all the values are the same because, if the priorities are identical, the bridge's MAC address is used to make the decision. Even though an entire 16-bit parameter is available for configuring a parameter, special care should be taken where newer versions of the rapid or multiple spanning tree protocol are involved. The priority value should only be changed in increments of 4096, because the lower 12 bits are used for other purposes. This could mean that these values may be ignored by future firmware releases.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

0 … 65535

Default:

32768

2.20.20.5 Max-Age

This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'outdated'. This defines how quickly the spanning-tree algorithm reacts to changes, for example due to failed bridges.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

1 … 65535 Seconds

Default:

20

2.20.20.6 Hello-Time

The Hello Time specifies the time interval (in seconds) for sending root-bridge information to the LAN. Note that the non-root bridge can adopt values from the root bridge. This value might be ignored depending on the topology of the network.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

1 … 32768 Seconds

Default:

2

2.20.20.7 Forward delay

This value determines the time (in seconds) that passes before a port should change from 'listening' to 'learning' or from 'learning' to 'forwarding'. However, now that rapid spanning tree offers a method of determining when a port can be

switched into the "forwarding state" without a long wait, this setting in many cases no longer has any effect. Do not change this value without detailed knowledge of spanning tree, since it may increase the risk of temporary loops in the network.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

1 … 32768 Seconds

Default:

6

2.20.20.11 Port data

This table can be used to set further spanning-tree parameters for each port.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

2.20.20.11.2 Port

The name of the LAN interface.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree** > **Port-Data**

2.20.20.11.4 Priority

The priority of the port set as an 8-bit value. If more than one port is available as a path to a LAN and the distance to both ports is the same, then this value decides which port is to be selected. If two ports have the same priority, then the port with the smaller number is selected.

Rapid spanning tree uses only the upper 4 bits of this value, for example, if a value is increased and decreased in 16 steps. Lower values take a higher priority.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree** > **Port-Data**

Possible values:

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

Default:

128

2.20.20.11.6 Edge port

A port can be labeled as an edge port.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree** > **Port-Data**

Possible values:

No
Yes

Default:

No

2.20.20.11.7 Path cost override

Specifies the influence of path cost.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree** > **Port-Data**

Possible values:

0 … 4294967295

Default:

0

2.20.20.12 Protocol version

This item selects the spanning-tree protocol version to be used. Setting this switch to 'Classic' will engage the algorithm defined in IEEE 802.1D-1998 chapter 8, while setting it to 'Rapid' will engage the rapid spanning three scheme defined by IEEE 802.1D-2004 chapter 17.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

Classic
Rapid

Note the upward compatibility of this protocol. Rapid spanning tree will automatically fall back to classic spanning tree data elements and schemes if other bridges are detected that do not support rapid spanning tree.

Default:

Classic

2.20.20.13 Transmit-Hold-Count

Determines the number of BPDUs (Bridge Protocol Data Units) that may be sent when using rapid spanning tree, before a second break is inserted. (With classic spanning tree, this value has no effect.)

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

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

Default:

6

2.20.20.14 Path cost computation

This item sets the protocol to be used for calculating the path cost. While the rapid spanning tree method uses the full 32-bit value range, the classic algorithm only works with a 16-bit value range. The rapid spanning tree method is only useful if it is supported by all bridges in the network and it is consistently configured.

Console path:

Setup > **LAN-Bridge** > **Spanning-Tree**

Possible values:

Classic
Rapid

Default:

Classic

2.20.30 IGMP-snooping

This menu contains the configuration options for IGMP/MLD snooping.

Console path:

Setup > **LAN-Bridge**

2.20.30.1 Operating

Activates or deactivates IGMP/MLD snooping in the device and all of the defined querier instances. Without IGMP/MLD snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

If this function is deactivated, the bridge sends all IP multicast packets on all ports. With a change of the operating mode, the device completely resets the IGMP/MLD snooping function, i.e. it deletes all dynamically learned values (memberships, router-port properties).

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

No
Yes
Auto

Default:

Auto

2.20.30.2 Port-settings

This table defines the port-related settings for IGMP/MLD snooping.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

2.20.30.2.1 Port

From the list of ports available on the device, select the port to which the settings relate.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Port-Settings**

2.20.30.2.2 Router-port

This option defines the port's behavior.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Port-Settings**

Possible values:

No

This port will never work as a router port, irrespective of IGMP/MLD queries or router messages received on this port.

Yes

This port will always work as a router port, irrespective of IGMP/MLD queries or router messages received on this port.

Auto

This port will work as a router port if IGMP/MLD queries or router messages are received. The port loses this status if no packets are received for the duration of ""Robustness*Query-Interval+(Query-Response-Interval/2)".

Default:

Auto

2.20.30.3 Unregistered-Data-Packet-Handling

This setting defines the handling of multicast data packets with a destination address outside of the reserved ranges "224.0.0.x" and "FF02::1", for which neither static memberships were defined nor were dynamic memberships learned.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

Router-Ports-only
Sends these packets to all router ports.

Flood
Sends these packets to all ports.

Discard
Discards these packets.

Default:

Router-Ports-only

2.20.30.4 Simulated-queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP/MLD snooping functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

2.20.30.4.1 Name

Name of the querier instance

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Simulated-Queriers**

Possible values:

Max. 8 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.20.30.4.2 Operating

Name of the querier instance

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Simulated-Queriers**

Possible values:

No
Yes

Default:

No

2.20.30.4.3 Bridge-group

Limits the querier instance to a certain bridge group.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Simulated-Queriers**

Possible values:

BRG-1
BRG-2
BRG-3
BRG-4
BRG-5
BRG-6
BRG-7
BRG-8
None

With this setting, the IGMP queries are issued on all bridge groups.

Default:

BRG-1

2.20.30.4.4 VLAN-ID

Limits the querier instance to a certain VLAN.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Simulated-Queriers**

Possible values:

0 … 4096

Default:

0

Special values:

0

If "0" is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

2.20.30.4.6 Protocol

Limits the querier instance to a certain protocol.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Simulated-Queriers**

Possible values:

IGMP
MLD

2.20.30.5 Query-Interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP/MLD queries to the multicast address 224.0.0.1 or FF02::1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships "age", expire, and are then deleted.

After the startup phase, the querier sends IGMP/MLD queries in this interval.

A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

The query interval must be greater than the query response interval.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

Max. 10 characters from `[1-9]`

Default:

125

2.20.30.6 Query-Response-Interval

Interval in seconds influencing the timing between IGMP/MLD queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP/MLD queries. These regular queries influence the time in which memberships "age", expire, and are then deleted.

The query response interval must be less than the query interval.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

Max. 10 characters from `[1-9]`

Default:

10

2.20.30.7 Robustness

This value defined the robustness of the IGMP/MLD protocol. This option tolerates packet losses of IGMP/MLD queries with respect to Join messages.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

Max. 10 characters from `[1-9]`

Default:

2

2.20.30.8 Static-Members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

2.20.30.8.1 Address

The IP address of the manually defined multicast group.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Static-Members**

Possible values:

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

2.20.30.8.2 Static-Members

These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received. They are specified as as a comma-separated list of the required ports.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Static-Members**

Possible values:

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

Default:

empty

2.20.30.8.3 VLAN-ID

The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Static-Members**

Possible values:

0 … 4096

Default:

0

Special values:

0

If "0" is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

2.20.30.8.4 Allow-Learning

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping** > **Static-Members**

Possible values:

Yes
No

Default:

Yes

2.20.30.9 Advertise-Interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP/MLD snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP/MLD queries.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

4 … 180 Seconds

Default:

20

2.20.30.10 Protocols

Specify the supported protocols: IGMP, MLD, or both.

Console path:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Possible values:

IGMP
MLD
IGMP and MLD

2.20.40 DHCP-Snooping

Here you can configure DHCP snooping for each interface.

Console path:

Setup > **LAN-Bridge**

2.20.40.1 Port

Indicates the physical or logical interface to which this DHCP-snooping configuration applies.

Console path:

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

Possible values:

LAN-x
All physical LAN interfaces

WLAN-x
All physical WLAN interfaces

WLAN-x-x
All logical WLAN interfaces

P2P-x-x
All logical P2P interfaces

WLC-TUNNEL-x
All virtual WLC tunnels

2.20.40.2 Add agent info

Here you decide whether the DHCP relay agent appends incoming DHCP packets with the DHCP option "relay agent info" (option 82), or modifies an existing entry, before forwarding the request to a DHCP server.

This option allows the relay agent to deliver additional information to the DHCP server about the interface used by the client to make the request.

The "relay agent info" is composed of values for the **Remote ID** and the **Circuit ID**.

If these two fields are empty, the DHCP relay agent does not add any 'Relay Agent Info' to the data packets.

Console path:

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

Possible values:

Yes
Adds "relay agent info" to the DHCP packets.

No
This setting disables DHCP snooping for this interface.

Default:

No

2.20.40.3 Treat-Existing-Agent-Info

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets.

Console path:

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

Possible values:

Keep
In this setting, the DHCP relay agent forwards a DHCP packet and any existing "relay agent info" unchanged to the DHCP server.

Replace

In this setting, the DHCP relay agent replaces any existing "relay agent info" with the values specified in the fields **Remote ID** and **Circuit ID**.

Drop

In this setting, the DHCP relay agent deletes any DHCP packet containing "relay agent info".

Default:

Keep

2.20.40.4 Remote ID

The remote ID is a sub-option of the "Relay agent info" option. It uniquely identifies the client making a DHCP request.

You can use the following variables:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%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**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

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

Possible values:

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

Default:

empty

2.20.40.5 Circuit ID

The circuit ID is a sub-option of the "Relay agent info" option. It uniquely identifies the interface used by the client to make a DHCP request.

You can use the following variables:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%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**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

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

Possible values:

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

Default:

empty

2.20.41 DHCPv6-Snooping

This is where you can configure the lightweight DHCPv6 relay agent.

Console path:

Setup > **LAN-Bridge**

2.20.41.1 Port

Indicates the physical or logical interface to which this DHCPv6-snooping configuration applies.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

LAN-x
All physical LAN interfaces

WLAN-x
All physical WLAN interfaces

WLAN-x-x
All logical WLAN interfaces

P2P-x-x

All logical P2P interfaces

WLC-TUNNEL-x

All virtual WLC tunnels

2.20.41.2 Orientation

Enable or disable DHCPv6 snooping here.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

Network-Facing

Disables DHCPv6 snooping for this interface. The LDRA does not forward any DHCPv6 requests to a DHCPv6 server.

Client-Facing:

Enables DHCPv6 snooping for this interface.

Default:

Network-Facing

2.20.41.3 Type

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

Trusted

The LDRA forwards DHCP requests from clients and also DHCP responses from DHCP servers.

Untrusted

If this interface is classified as untrusted, the LDRA discards DHCPv6-server requests to this interface. This prevents unauthorized clients from acting as "rogue DHCPv6 servers". Similarly, the LDRA does not forward DHCPv6 responses with the wrong interface ID to the client.

Interfaces that are facing clients should be set as untrusted.

Default:

Trusted

2.20.41.4 Remote ID

According to RFC 4649, the remote ID uniquely identifies the client making a DHCPv6 request.

This option is analogous to the DHCP option "Remote ID" of the relay agent in IPv4.

You can use the following variables:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%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**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

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

Default:

empty

2.20.41.5 Interface-Id

The interface ID uniquely identifies the interface used by a client to make a DHCPv6 request.

You can use the following variables:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%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**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.

- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

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

Default:

empty

2.20.41.6 Server address

You can set the IPv6 address of a DHCPv6 server here.

Leave this field blank if you want to receive responses from all DHCPv6 servers on the network. Otherwise the LDRA reacts only to DHCPv6 responses from the server you have specified. In this case, the LDRA discards responses from other DHCPv6 servers.

Console path:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Possible values:

Max. 39 characters `0123456789ABCDEFabcdef:.`

Default:

empty

2.20.42 RA-Snooping

You can configure the RA snooping here.

Console path:

Setup > **LAN-Bridge**

2.20.42.1 Port

Indicates the physical or logical interface to which this RA-snooping configuration applies.

Console path:

Setup > **LAN-Bridge** > **RA-Snooping**

Possible values:

LAN-x
All physical LAN interfaces
WLAN-x
All physical WLAN interfaces
WLAN-x-x
All logical WLAN interfaces
P2P-x-x
All logical P2P interfaces
WLC-TUNNEL-x
All virtual WLC tunnels

2.20.42.3 Orientation

Specify the preferred interface type here.

Console path:

Setup > **LAN-Bridge** > **RA-Snooping**

Possible values:

Router
The device mediates all of the RAs arriving at this interface.
Client
The device discards all of the RAs arriving at this interface.

Default:

Router

2.20.42.4 Router-Address

If you have selected the interface type **Router**, enter an optional router address here. If you specify a router address, the device will only mediate RAs from that router. With the interface type **Client** selected, the device ignores this input field.

Console path:

Setup > **LAN-Bridge** > **RA-Snooping**

Possible values:

Max. 39 characters `0123456789ABCDEFabcdef:.`

Default:

empty

2.20.43 PPPoE snooping

Here you configure PPPoE snooping for each interface.

Console path:

Setup > **LAN-Bridge**

2.20.43.1 Port

Indicates the physical or logical interface to which this PPPoE-snooping configuration applies.

Console path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

LAN-x
All physical LAN interfaces

WLAN-x
All physical WLAN interfaces

WLAN-x-x
All logical WLAN interfaces

P2P-x-x
All logical P2P interfaces

WLC-TUNNEL-x
All virtual WLC tunnels

GRE-TUNNEL-x
All virtual GRE tunnels

2.20.43.2 Add agent info

Here you decide whether the PPPoE intermediate agent gives incoming PPPoE packets a manufacturer-specific PPPoE tag with the vendor ID "3561" before forwarding the request to a PPPoE server.

This option allows the PPPoE intermediate agent to deliver additional information to the PPPoE server about the interface used by the client to make the request.

The PPPoE tag is composed of values for the **Remote ID** and the **Circuit ID**.

If these two fields are empty, the PPPoE intermediate agent does not add a PPPoE tag to the data packets.

Console path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Yes
Adds "relay agent info" to the PPPoE packets.

No

This setting disables PPPoE snooping for this interface.

Default:

No

2.20.43.3 Remote ID

The remote ID is a sub-option of the PPPoE intermediate agent option. It uniquely identifies the client making a PPPoE request.

You can use the following variables:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%c`: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- `%n`: Inserts the name of the PPPoE intermediate agent as specified under **Setup** > **Name**.
- `%v`: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

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

Default:

empty

2.20.43.4 Circuit ID

The circuit ID is a sub-option of the PPPoE intermediate agent info option. It uniquely identifies the interface used by the client to make a PPPoE request.

You can use the following variables:

- `%%`: Inserts a percent sign.

- `%c`: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%c`: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- `%n`: Inserts the name of the PPPoE intermediate agent as specified under **Setup** > **Name**.
- `%v`: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

Console path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

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

Default:

empty

2.20.43.5 Discard server packets

Here you decide whether the PPPoE intermediate agent retains or discards any existing PPPoE tags.

Console path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Yes

The PPPoE intermediate Agent removes existing PPPoE tags and leaves both the “Circuit ID” and the “Remote ID” empty.

No

The PPPoE intermediate agent takes over any existing PPPoE tags.

Default:

No

2.21 HTTP

This menu contains the HTTP settings.

Console path:

Setup

Possible values:

4 … 180 Seconds

Default:

20

2.21.1 Document root

This parameter defines the path to a directory where the help for WEBconfig is stored locally.

Console path:

Setup > **HTTP**

Possible values:

Max. 99 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.21.2 Page headers

Use this setting to choose whether the page headers of the HTTP pages for the Public Spot should be displayed as text or as images.

The settings for the page headers are intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **HTTP**

Possible values:

Images
Texts

Default:

Images

2.21.3 Font family

Font family for Web interface display.

Console path:

Setup > **HTTP**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

helvetica,sans-serif

2.21.5 Page headers

Select here whether the Public Spot displays the page headers of the standard pages as text or graphics.

Console path:

Setup > **HTTP**

Possible values:

Images
Texts

Default:

Images

2.21.6 Error page style

Normal error display or bluescreen

Console path:

Setup > **HTTP**

Possible values:

Standard
Nifty

Default:

Standard

2.21.7 Port

Port for the HTTP server connection.

Console path:

Setup > **HTTP**

Possible values:

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

Default:

80

2.21.9 Max-Tunnel-Connections

The maximum number of simultaneously active HTTP tunnels

Console path:

Setup > **HTTP**

Possible values:

1 … 255

Default:

3

2.21.10 Tunnel-Idle-Timeout

Life-expectancy of an inactive tunnel. After expiry of this time period the tunnel closes automatically unless data transfer is actively taking place.

Console path:

Setup > **HTTP**

Possible values:

1 … 4294967295 Seconds

Default:

300

2.21.11 Session timeout

Period of validity (lease) for the WEBconfig session without user activity, in seconds. When this period expires the password must be reentered.

Console path:

Setup > **HTTP**

Possible values:

1 … 4294967295 Seconds

Default:

600

2.21.13 Standard design

Selects the design that will be used by default to display WEBconfig.

Console path:

Setup > **HTTP**

Possible values:

Normal_design
Design_for_small_resolutions
Design_for_high_contrast

Default:

Normal_design

2.21.14 Show device information

This table defines the system information that is displayed on the System data/ Device status page in WEBconfig.

Console path:

Setup > **HTTP**

2.21.14.1 Device-information

Selection of device information to be displayed in WEBconfig.

Console path:

Setup > **HTTP** > **Show-device-information**

Possible values:

CPU
Memory
UMTS/Modem-Interface
Ethernet ports
P2P connections
Throughput(Ethernet)
Router
Firewall
DHCP
DNS
VPN
Connections
Time
IPv4 addresses
IPv6 addresses
IPv6 prefixes
DHCPv6 client
DHCPv6 server
Operating-Time
ADSL
ISDN
DSLoL

2.21.14.2 Position

Index for the sequence for the display of device information.

Console path:

Setup > **HTTP** > **Show-device-information**

Possible values:

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

Default:

0

2.21.14.2 Position

The contents of WEBconfig are compressed in order to speed up the display. The compression can be deactivated for browsers that do not support it.

Console path:

Setup > **HTTP**

Possible values:

Operating
Only_for_WAN
Deactivated

Default:

Operating

2.21.16 Keep-Server-Ports-Open

This menu contains the parameters for restricting access to the web server services.

Console path:

Setup > **HTTP**

2.21.16.1 Ifc.

Here, the settings for access to the web-server services can be adjusted for each of the access interfaces available on the device (model dependent, e.g. LAN, WAN, WLAN).

Console path:

Setup > **HTTP** > **Keep-Server-Ports-Open**

2.21.16.2 Keep-Server-Ports-Open

You can decide whether access to the device configuration via HTTP is to be enabled, disabled or limited to read-only. Irrespective of this, access to the web server services can be regulated separately, e.g. to enable communication via CAPWAP, SSL-VPN or SCEP-CA via HTTP(S), even if HTTP(S) has been disabled.

For each access method (LAN, WAN, WLAN, depending on the device), you set the access rights for the device's web server services at the HTTP server port.

The default is for

- LAN and WLAN automatic and
- disabled for WAN.

Console path:

Setup > **HTTP** > **Keep-Server-Ports-Open**

Possible values:

Automatic

The HTTP server port is open, as long as a service is registered (e.g. CAPWAP). If no service is registered, the server port will be closed.

Activated

The HTTP server port is always open, even if access to the configuration with HTTP is disabled. This can be used to restrict direct access to the configuration. However, the automatic configuration of APs by a WLAN controller is still possible.

Disabled

The HTTP server port is closed and no service can use the web server. If access to the configuration via HTTP is enabled, then a message is displayed expressing that the web server is not available.

2.21.20 Rollout-Wizard

This menu contains the settings for the Rollout Wizard.

Console path:

Setup > **HTTP**

2.21.20.1 Operating

Switches the Rollout Wizard on or off. After being switched on the Wizard appears as an option on the WEBconfig start page.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

Possible values:

No
Yes

Default:

No

2.21.20.2 Title

The name for the Rollout Wizard as displayed in the navigation tree in WEBconfig under **Setup Wizards**.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

Possible values:

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

Default:

Rollout

2.21.20.8 Use extra checks

This option enables consistency tests that check some internal aspects of the wizard.

Executing these additional tests is very time consuming. Activate this option only during development of the wizard and deactivate this option for normal operation.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

Possible values:

No
Yes

Default:

No

2.21.20.9 Presets

This table enables you to predefine the values for all of the parameters that are requested by the Default Rollout Wizard. Parameters configured in this way are no longer queried when you run the Default Rollout Wizard.

A 'blank' predefined value for **Port** and for **Source loopback address** will be interpreted by the device as the entry 'Auto'. In this case, the Default Rollout Wizard uses the corresponding HTTP(S) standard port and, as the loopback address, the address of your device that matches to the target. If you are working with different ARF networks, you must use the loopback address to specify the ARF where the LSR server is located.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

2.21.20.9.1 Name

This entry shows the name of the parameter that can be filled with preset values.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **Presets**

2.21.20.9.2 Preset

This entry shows the preset value for the corresponding parameter in the Rollout Wizard.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **Presets**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.21.20.9.3 Use preset

This entry defines whether the parameter value configured here is to be used by the Rollout Wizard. If set to yes, the Rollout Wizard will no longer query this parameter.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **Presets**

Possible values:

No
Yes

Default:

No

2.21.20.10 Delete Wizard

This action deletes a user-defined Rollout Wizard. When you enable the Rollout Wizard in future, the device uses the internal LCOS default wizard.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

2.21.20.11 SSL

This menu contains the SSL configuration for the Rollout Wizard.

Console path:

Setup > **HTTP** > **Rollout-Wizard**

2.21.20.11.1 Versions

Here you select the encryption version(s) to be used.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.21.20.11.2 Key-exchange algorithms

Here you select the algorithms to be used for the key exchange.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.21.20.11.3 Crypto algorithms

Here you select the encryption algorithms to be used.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.21.20.11.4 Hash algorithms

Here you select the hash algorithms to be used.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

MD5
SHA1
SHA-256
SHA-384
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA-256

SHA-384

SHA2-256

SHA2-384

2.21.20.11.5 Prefer PFS

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

To disable this function, uncheck the box.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

Yes

Default:

Yes

2.21.20.11.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

Forbidden

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

Allowed

The device permits renegotiations with the remote station.

Ignored

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

Default:

Allowed

2.21.20.11.7 Elliptic curves

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

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.21.20.11.21 Signature hash algorithms

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

Console path:

Setup > **HTTP** > **Rollout-Wizard** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.21.21 Max-HTTP-Job-Count

Using this setting you specify the maximum number of HTTPS jobs. An HTTP job exists when LCOS is serving an HTTP connection from a client, for example in the form of a request to WEBconfig. The setting therefore defines the maximum number of concurrent HTTP connections.

Console path:

Setup > **HTTP**

Possible values:

5 … 512

Default:

Depends on device

2.21.22 Disable-Password-Autocompletion

This switch controls whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

Console path:

Setup > **HTTP**

Possible values:

No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

Yes

The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

Default:

No

2.21.24 Automatic-Redirect-to-HTTPS

This switch determines whether the WEBconfig login dialog receiving an unencrypted connection request automatically switches to an encrypted HTTPS connection. This is always switched on in new configurations. Existing configurations will not be changed.

Console path:

Setup > **HTTP**

Possible values:

No

WEBconfig does not automatically switch to an encrypted connection upon receiving an unencrypted connection request.

Yes

WEBconfig automatically switches to an encrypted connection upon receiving an unencrypted connection request.

Default:

Yes

2.21.30 File server

This menu contains the file-server settings for external USB data media.

Console path:

Setup > **HTTP**

2.21.30.1 Public-Subdir

This directory is the root directory on a USB medium. The device ignores all other files on the USB medium.

Console path:

Setup > **HTTP** > **File-Server**

Possible values:

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

Default:

public_html

2.21.30.2 Operating

This parameter activates or deactivates the file server for USB media.

Console path:

Setup > **HTTP** > **File-Server**

Possible values:

Yes
No

Default:

Yes

2.21.40 SSL

The parameters for HTTPS connections are specified here.

Console path:

Setup > **HTTP**

2.21.40.3 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.21.40.4 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.21.40.5 Crypro algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

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

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.21.40.6 Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.21.40.7 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

On
Off

Default:

On

2.21.40.8 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **HTTP** > **SSL**

Possible values:

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

Allowed
The device permits renegotiations with the remote station.

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

Default:

Allowed

2.21.40.9 Elliptic curves

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

Console path:

Setup > **HTTP** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.21.40.10 Port

Port for the HTTPS server connection

Console path:
Setup > **HTTP** > **SSL**

Possible values:
0 … 65535

Default:
443

2.21.40.11 Use-User-Provided-Certificate

Here you select whether you want to use a user-provided certificate.

Console path:
Setup > **HTTP** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.21.40.23 Signature hash algorithms

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

Console path:

Setup > **HTTP** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.21.50 Start-TCP-HTTP-Tunnel

With this action, you can create a TCP-/HTTP tunnel.

Console path:

Setup > **HTTP**

Possible arguments:

-r
Routing tag.

-h
Host address to be accessed via the tunnel.

-p
Local port.

-a
Optional remote address.

2.22 SYSLOG

This menu contains the SYSLOG settings.

Console path:

Setup

2.22.1 Operating

Activates the dispatch of information about system events to the configured SYSLOG client.

Console path:

Setup > **SYSLOG**

Possible values:

Yes
No

Default:

Yes

2.22.2 SYSLOG table

This table defines the SYSLOG clients.

Console path:

Setup > **SYSLOG**

Possible values:

Yes
No

Default:

Yes

2.22.2.1 Idx.

Position of the entry in the table.

Console path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

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

Default:

empty

2.22.2.3 Source

Here you select which source is entered in the SYSLOG messages.

Console path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

None
System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

None

2.22.2.4 Level

Here you select the source that is entered in the SYSLOG messages. Multiple entries can be selected.

Console path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

2.22.2.6 Loopback-Addr.

Sender address entered into the SYSLOG message. No answer is expected to a SYSLOG message.

Console path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.

2.22.2.7 IP address

Contains the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a DNS name.

Console path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

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

2.22.2.8 Port

This entry contains the port used for SYSLOG.

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

514

TCP/UDP

Default:

514

2.22.2.9 Protocol

Specifies which transport protocol the syslog client should use for sending syslog messages to the server.

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

TCP

Transmission Control Protocol

UDP

User Datagram Protocol

TLS

The syslog client supports three scenarios in TLS mode:

1. The syslog client accepts all TLS server certificates from the syslog server. For this purpose, no trusted CA certificate is stored in the router.
2. The syslog client only accepts server certificates signed by a trusted CA. To do this, the CA certificate must be uploaded to the corresponding certificate slot on the router.
3. The syslog client authenticates itself with the syslog server using a TLS client certificate and the syslog server authenticates itself with its CA certificate. To do this, both the TLS client certificate for the router and the CA certificate must be uploaded to the corresponding certificate slot on the router, e.g. in a container as a PKCS#12 file.

Default:

UDP

2.22.2.10 Filter-Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the field **Filter name**, are allowed or denied.

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

Allow
Deny

Default:

Deny

2.22.2.11 Filter-Name

References a SYSLOG filter.

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

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

2.22.2.12 RFC5424-Format

Specifies whether the syslog client should send messages to the syslog server in RFC5424 format.

Console path:

Setup > **SYSLOG** > **Server**

Possible values:

Yes
No

Default:

No

2.22.3 Facility-Mapper

This table defines the allocation of SYSLOG sources to facilities.

Console path:

Setup > **SYSLOG**

2.22.3.1 Source

The mapping of sources to specific facilities.

Console path:

Setup > **SYSLOG** > **Facility-Mapper**

Possible values:

System
Logins
System time
Console login
Connections
Accounting
Administration
Router

2.22.3.2 Facility

The mapping of sources to specific facilities.

Console path:

Setup > **SYSLOG** > **Facility-Mapper**

Possible values:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

2.22.4 Port

Port used for sending SYSLOG messages.

Console path:

Setup > **SYSLOG**

Possible values:

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

Default:

514

2.22.5 Messages-Table-Order

This item determines the order in which the messages table is displayed.

Console path:

Setup > **SYSLOG**

Possible values:

Oldest on top
Newest on top

Default:

Newest on top

2.22.6 Backup interval

This parameter defines the interval in hours for the boot-persistent storage of SYSLOG messages to the flash memory of the device.

Console path:

Setup > **SYSLOG**

Possible values:

1 … 99 Hours

Default:

2

2.22.7 Backup active

Enables the boot-persistent storage of SYSLOG messages to the flash memory of the device.

Console path:

Setup > **SYSLOG**

Possible values:

No
Yes

Default:

Yes

2.22.8 Log-CLI-Changes

This parameter enables logging of the commands entered on the command line. Enable this parameter to log an entry in the internal SYSLOG memory when a command is entered on the command line of the device.

This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

Console path:

Setup > **SYSLOG**

Possible values:

No
Yes

Default:

No

2.22.9 Max-Message-Age

This parameter defines the maximum period for retaining SYSLOG messages in the internal SYSLOG memory of the device in hours. After this period expires the device automatically deletes the obsolete SYSLOG messages if auto-delete is activated under *2.22.10 Remove-Old-Messages* on page 690.

Console path:

Setup > **SYSLOG**

Possible values:

1 … 99 Hours

Default:

24

2.22.10 Remove-Old-Messages

This parameter enables deletion of the SYSLOG messages in the device after the period set for *2.22.9 Max-Message-Age* on page 690.

Console path:

Setup > **SYSLOG**

Possible values:

No
Yes

Default:

No

2.22.11 Max. age unit

This parameter determines whether the message age is specified in hours, days and months.

In this case, a month is 30 days.

Console path:

Setup > **SYSLOG**

Possible values:

Hour
Day
Month

Default:

Hour

2.22.12 Critical prio

With this setting you define the lowest syslog priority considered by the device to be 'critical'. As of this priority level, the device generates the corresponding alerts that you recieve, for example, in WEBconfig.

Console path:

Setup > **SYSLOG**

Possible values:

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Default:

Critical

2.22.13 Filter

This table is used to define the filter rules.

Console path:

Setup > **SYSLOG**

2.22.13.1 Idx.

Position of the entry in the table.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

Max. 4 characters from `[A_Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.22.13.2 Filter-Name

The name of the filter rule; the server table references this name. Several rules can be created with the same filter name. When messages are sent, these rules are checked in the order of their position in the filter table. If there is no matching rule in this filter chain, the message is sent or discarded according to the server's default policy in the server table.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

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

2.22.13.3 Match-source

Source of the message to which this rule applies. The value “none” stands for any source.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

None
System
Login
System time
CLI login
Connections
Accounting
Administration
Router

Default:

None

2.22.13.4 Match-level

Priority of the message to which this rule applies. The value “none” stands for any priority.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

2.22.13.5 Filter-Regex

Regular expression in Perl syntax to which the message text must apply. An empty string means that the message text is ignored, and therefore all message texts apply.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

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

2.22.13.6 Set-source

New source of the message if the rule applies. The value “none” means that the source is not changed.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

None
System
Login
System time
CLI login
Connections
Accounting
Administration
Router

Default:

None

2.22.13.7 Set-level

New priority of the message if the rule applies. The value “None” means that the priority is not changed.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

2.22.13.8 Filter-Action

Action if the rule applies. Either allow or deny sending the message to the server.

Console path:

Setup > **SYSLOG** > **Filter**

Possible values:

Allow
Deny

Default:

Deny

2.23 Interfaces

This menu contains the settings for the interfaces.

Console path:

Setup

2.23.1 S0

This item allows you to make further settings for the device interface.

Console path:

Setup > **Interfaces**

2.23.1.1 Ifc

Select the device ISDN interface which the settings relate to, e.g. S0-1 or S0-2.

Console path:

Setup > **Interfaces** > **S0**

2.23.1.2 Protocol

This item allows you to select the D-channel protocol for this interface.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

No
DSS1
1TR6
P2P-DSS1
GRP0
Auto

Default:

Auto

2.23.1.7 LL B-channel

This item allows you to set the leased-line channel if the device is operated with a **Group 0**-type leased-line connection.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

None
B1
B2

Default:

None

2.23.1.9 Dial prefix

The number entered here will be placed in front of all telephone numbers making outgoing calls.

This is useful, for example, if your device is operated in a PBX that requires an outside-line access code. This number should be entered here.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

Max. 8 characters from `[0-9]`

Default:

empty

2.23.1.13 Max-in-calls

This setting allows you to place a limit on the number of concurrent calls that can be made over this interface. One advantage of this is that you can always leave a line free for other devices.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

None
One
Two

Default:

Two

2.23.1.14 Max-out-calls

This setting allows you to place a limit on the number of concurrent calls that can be made over this interface. One advantage of this is that you can always leave a line free for other devices.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

None
One
Two

Default:

Two

2.23.1.27 Termination

This entry determines whether the selected interface is terminated.

Console path:

Setup > **Interfaces** > **S0**

Possible values:

No
Yes

Default:

Yes

2.23.4 DSL

The settings for the DSL interface are located here.

Console path:

Setup > **Interfaces**

2.23.4.1 Ifc

Select the interface which the settings relate to, e.g. DSL, DSLoL, ADSL or VDSL.

The selection options depend on the equipment of the device.

Console path:

Setup > **Interfaces** > **DSL**

2.23.4.2 Operating

Here you can specify whether the interface is active or not.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

No
Yes

Default:

No

2.23.4.6 Mode

This item selects the mode in which the WAN interface is operated. In automatic mode, all PPPoE frames and all data packets belonging to a connection established over the DSLoL interface (as configured in the IP parameter list) are routed via the DSLoL interface (WAN). All other data packets are treated as normal LAN packets. In exclusive mode, the LAN interface operates as a WAN interface only.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

Auto
Exclusive

Default:

Exclusive

2.23.4.16 Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

empty

Special values:

0

No limitation on the amount of data transferred.

2.23.4.17 Ext.-Overhead

The external overhead results from the data that the modem attaches to each packet. For PPPoE connections, this is 4 bytes for the LLC header and 8 bytes for the AAL 5 trailer. The modem cannot send "partial" ATM cells, so on average half an ATM cell (= 24 bytes) must be allowed for additionally. The resulting total overhead is thus 36 bytes per transmitted packet.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

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

Default:

empty

2.23.4.18 Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN Ethernet. For example, on a T-DSL connection with guaranteed 768 kbit downstream, the upstream rate negotiated by the modem is 864 kbit. This still includes an overhead typical for this type of connection, which results from the modem using ATM as

the transport protocol. If we adjust the 864 kbit to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbit gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

empty

Special values:

0

No restriction on the received data traffic.

2.23.4.23 LAN Ifc

Select the LAN interface that the DSLoL interface is linked with. If an interface in entered multiple times, they are numbered consecutively.

Console path:

Setup > **Interfaces** > **DSL**

Possible values:

LAN-1
WLAN-1
P2P-1
BRG-1
GRE-TUNNEL-1
BUNDLE
L2TP-ETHERNET
BRG-1
Any

Default:

LAN-1

2.23.6 ADSL interface

The settings for the ADSL interface are located here.

Console path:

Setup > **Interfaces**

2.23.6.1 Ifc

Select the relevant interface here.

The selection options depend on the equipment of the device.

Console path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

ADSL
S0-1
DSL-1
DSL-2
DSL-3
UMTS

2.23.6.2 Protocol

Select the protocol that you want to use for this interface.

With ADSL multimode, the protocols G.DMT, T1.413 and G. Lite are all tried in sequence. Auto mode first attempts to connect using the ADSL2+ protocol. If no connection can be made, the system falls back successively to ADSL2 or G.DMT.

Console path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

No
Auto
ADSL2+
ADSL2
ADSL-Multimode
Annex-M-Auto
G.Dmt
T1.413

Default:

No

2.23.6.16 Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

Console path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

2.23.6.18 Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

Console path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

2.23.7 Modem-Mobile

The settings for the mobile-telephony modem are located here.

Console path:

Setup > **Interfaces**

2.23.7.1 Ifc

Here you select the interface which you want to configure.

The selection options depend on the equipment of the device.

Console path:

Setup > **Interfaces** > **Modem-Mobile**

Possible values:

DSL-1
EXT
ADSL
S0-1
DSL-1
DSL-2
DSL-3
UMTS

2.23.7.2 Operating

Select the operating mode for the interface.

Console path:

Setup > **Interfaces** > **Modem-Mobile**

Possible values:

No
Modem
WWAN
UMTS-GPRS

Default:

No

2.23.7.22 Profile

Here you select the profile to be used for the UMTS interface.

Console path:

Setup > **Interfaces** > **Modem-Mobile**

Possible values:

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

Default:

empty

2.23.8 VDSL

This menu contains the settings for the VDSL interface.

Console path:

Setup > **Interfaces**

2.23.8.1 Ifc

Name of the interface.

Console path:

Setup > **Interfaces** > **VDSL**

2.23.8.2 Protocol

This parameter specifies the protocol or standard used by the interface for data transmission.

Console path:

Setup > **Interfaces** > **VDSL**

Possible values:

Off

This setting disables the VDSL interface.

Auto

The device automatically selects the best transmission protocol.

VDSL

The device uses VDSL2 according to ITU-T G.993.2.

ADSL

ADSL2+

The device uses ADSL2+ according to ITU-T G.992.5.

ADSL2

The device uses ADSL2 according to ITU-T G.992.3.

ADSL1

The device uses ADSL1 according to ITU-T G.992.1 or G.DMT.

ADSL2+J

The device uses ADSL2+ according to ITU-T G.992.5 Annex J.

ADSL2J

The device uses ADSL2+ according to ITU-T G.992.3 Annex J.

Default:

Auto

2.23.8.16 Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

Console path:

Setup > **Interfaces** > **VDSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

2.23.8.18 Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

Console path:

Setup > **Interfaces** > **VDSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

2.23.8.25 Handshake

This entry sets the data-flow control to be used for VDSL.

Console path:

Setup > **Interfaces** > **VDSL**

Possible values:

Chipset-default
V43 if needed
V43 enabled
V43 disabled

Default:

Chipset-default

2.23.8.28 Options

This entry sets the options to be used for VDSL. You can enable or disable retransmission and virtual noise for the upstream or downstream directions.

Retransmission is a feature for repairing a data connection. If an error occurs during the data transmission, the remote station resends the lost data. For this purpose, the sender briefly retains the sent data in memory and, if necessary, sends it to the requestor again.

Virtual noise is a feature that improves the stability of a VDSL line. It compensates for crosstalk between adjacent lines.

Console path:

Setup > **Interfaces** > **VDSL**

Possible values:

No-Options
All options disabled.

DS-ReTx
Enable downstream retransmission.

US-ReTx
Enable upstream retransmission.

DS-VN
Enable virtual noise for downstream.

US-VN
Enable virtual noise for upstream.

Default:

DS-ReTx

DS-VN

US-VN

2.23.18 Permanent L1 activation

Permanent L1 activation prevents the S0 bus from being disabled, or it prevents a reactivation after a successful deactivation.

This setting is particularly relevant if you are using a bus as a PCM sync source. If the bus is disabled, you will lose the PCM clock.

Console path:

Setup > **Interfaces**

Possible values:

Disabled
Sync source only
All TE interfaces

2.23.19 PCM-SYNC-SOURCE

PCM sync source sets the S0-bus used as a clock by the Call Manager.

This setting is relevant if you use a bus internally and the second bus is connected externally (e.g. to a connection from the ISDN provider). In this case, you should use the external connection as the clock. With the setting **Auto** the device selects the bus by itself.

Console path:

Setup > **Interfaces**

Possible values:

Auto
S0-1

2.23.20 WLAN

This menu contains the settings for wireless LAN networks

Console path:

Setup > **Interfaces**

2.23.20.1 Network

Here you can adjust further network settings for each logical wireless LAN network (MultiSSID) supported by your device.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.1.1 Ifc

Select from the logical WLAN interfaces.

Console path:

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

2.23.20.1.2 Network name

Define a unique SSID (the network name) for each of the logical wireless LANs required. Only WLAN clients that have the same SSID can register with this wireless network.

Console path:

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

Possible values:

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

Default:

empty

2.23.20.1.4 Closed network

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in cleartext so that it is briefly visible to all clients in the WLAN network.

Console path:

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

Possible values:

No

The access point publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).

Yes

The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID.

Tightened

The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond.

Default:

No

2.23.20.1.8 Operating

Switches the logical WLAN on or off separately.

Console path:

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

Possible values:

Yes
No

Default:

Yes

2.23.20.1.9 MAC filter

The MAC addresses of the clients allowed to associate with an access point are stored in the MAC filter list. The **MAC filter** switch allows the use of the MAC filter list to be switched off for individual logical networks.

Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The MAC filter list is always consulted for registrations with an individual passphrase, even if this option is deactivated.

Console path:

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

Possible values:

Yes
No
Local only
RADIUS only

Default:

Yes

2.23.20.1.10 Max. stations

Here you set the maximum number of clients that may associate with this access point in this network. Additional clients wanting to associate will be rejected.

Console path:

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

Possible values:

0 … 65535

Default:

0

Special values:

0

Limitation switched off

2.23.20.1.11 Cl.-Brg.-Support

Whereas address adaptation allows only the MAC address of a single attached device to be visible to the access point, client-bridge support provides transparency in that all MAC addresses of the LAN stations behind the client stations are transferred to the access point.

Furthermore, the three MAC addresses usual in client mode are not used for this operating mode (in this example for server, access point and client station), but rather four addresses as with point-to-point connections (the fourth is the MAC address of the station in the LAN of the client station). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, initiated by a broadcast.

Client-bridge mode can only be used between two LANCOM devices.

Console path:

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

Possible values:

Yes

Activates client-bridge support for this logical WLAN.

No

Deactivates client-bridge support for this logical WLAN.

Exclusive

Only accepts clients that also support the client-bridge mode.

Default:

No

2.23.20.1.12 RADIUS accounting

Deactivates accounting via a RADIUS server for this network.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.1.13 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. Individual settings can be made for every logical WLAN as to whether clients in this SSID can exchange data with one another.

Console path:

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

Possible values:

No
Yes

Default:

Yes

2.23.20.1.14 APSD

Activates APSD power saving for this logical WLAN network.

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.1.15 Aironet extensions

Activates Aironet extensions for this logical wireless LAN.

Console path:

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

Possible values:

No
Yes

Default:

Yes

2.23.20.1.16 Min-Client-Strength

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

Console path:

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

Possible values:

0 … 100

Default:

0

2.23.20.1.17 Include UUID

Here you can determine whether the corresponding radio module should transfer its UUID.

Console path:

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

Possible values:

No
Yes

Default:

Yes

2.23.20.1.19 Transmit-only-Unicasts

Multicast and broadcast transmissions within a WLAN cell cause a load on the bandwidth of the cell, especially since the WLAN clients often do not know how to handle these transmissions. The access point already intercepts a large part of the multicast and broadcast transmissions in the cell with ARP spoofing. With the restriction to unicast transmissions it filters out unnecessary IPv4 broadcasts from the requests, such as Bonjour.

The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.1.20 Tx-Limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID.

Console path:

Setup > **Interfaces** > **WLAN**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

2.23.20.1.21 Rx-Limit

With this setting, you define the overall bandwidth that is available for reception within this SSID.

Console path:

Setup > **Interfaces** > **WLAN**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

2.23.20.1.22 Accounting server

Using this parameter, you define a RADIUS accounting server for the corresponding logical WLAN interface.

Console path:

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

Possible values:

Name from **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**

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

Default:

empty

2.23.20.1.23 Per-Client-Tx-Limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Console path:

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

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

2.23.20.1.24 Per-Client-Rx-Limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Console path:

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

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

2.23.20.1.25 LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

Console path:

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

Possible values:

No

LBS tracking is disabled.

Yes

LBS tracking is enabled.

2.23.20.1.26 LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

Console path:

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

Possible values:

Name from **Setup** > **WLAN** > **Network** > **LBS-Tracking**

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

Default:

empty

2.23.20.1.27 Accounting-Start-Condition

Use this entry to specify when the DHCP server reports the beginning of a billing period to a RADIUS accounting server.

Console path:

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

Possible values:

None

Accounting starts when the WLAN client takes on the status “Connected”.

Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6) from the DHCP server.

Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address from the DHCP server.

Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address from the DHCP server.

Default:

None

2.23.20.1.28 Dyn-Auth

This entry enables or disables dynamic authorization by RADIUS CoA on the corresponding interface.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.1.31 Timeframe

Select one of the time frames defined in *2.14.16 Timeframe* on page 478. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

Console path:

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

Possible values:

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

Default:

empty

2.23.20.1.32 Min-Client-Disassoc-Strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value *2.23.20.1.16 Min-Client-Strength* on page 712 is also set and the Min-Stations-Disassoc-Strength is less than this value.

Console path:

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

Possible values:

0 … 100

Default:

0

2.23.20.2 Transmission

Here you can adjust further transmission settings for each logical wireless LAN network (MultiSSID) supported by your device.

Console path:

Setup > **Interfaces** > **WLAN**

Possible values:

No
Yes

Default:

No

2.23.20.2.1 Ifc

Opens the settings for the available logical WLAN networks.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

No
Yes

Default:

No

2.23.20.2.2 Packet size

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

500 … 1600 Even values only

Default:

1600

2.23.20.2.3 Min-Tx-Rate

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum transmission speed if you wish to prevent the dynamic speed adjustment.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

2.23.20.2.4 Basic rate

The basic rate is the transmission rate with which the device sends all multicast and broadcast packets.

The basic rate set here should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached at this speed.

If you choose "Auto", the device automatically adapts to the transmission rate of the slowest WLAN client on your network.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

2M

2.23.20.2.6 RTS-Threshold

The RTS threshold uses the RTS/CTS protocol to prevent the occurrence of the "hidden station" phenomenon.

A collision between the very short RTS packets is improbable, although the use of RTS/CTS leads to an increase in overhead. The use of this procedure is only worthwhile where long data packets are being used and the risk of collision is higher. The RTS threshold is used to define the minimum packet length for the use of RTS/CTS. The best value can be found using trial and error tests on location.

The RTS threshold value also has to be set in the WLAN client, as far as the driver and/or operating system allow this.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

60 … 2347

Default:

2347

2.23.20.2.7 11b-Preamble

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
Long

Default:

Auto

2.23.20.2.9 Max-Tx-Rate

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The access point adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed value for the maximum transmission speed if you wish to prevent the dynamic speed adjustment.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

2.23.20.2.10 Min.-Frag.-Length

Packet fragment length below which fragments are dropped.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0 … 2347

Default:

16

2.23.20.2.11 Soft-Retries

If the hardware was unable to send a packet, the number of soft retries defines how often the system should attempt retransmission.

The total number of attempts is thus (soft retries + 1) * hard retries.

The advantage of using soft retries at the expense of hard retries is that the rate-adaption algorithm immediately begins the next series of hard retries with a lower data rate.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0 … 999

Default:

0

2.23.20.2.12 Hard-Retries

This value defines the number of times that the hardware should attempt to send packets before a Tx error message is issued. Smaller values mean that a packet which cannot be sent blocks the sender for less time.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0 … 15

Default:

10

2.23.20.2.13 Short guard interval

The default setting automatically optimizes the value for guard interval. If the momentary operating conditions allow, the interval will be set to the shortest possible value.

You also have the option is deactivating this mechanism to prevent the short-guard interval from being used.

Put simply, the guard interval reduces the signal distortion caused by intersymbol interference (ISI) when using signal multiplexing (OFDM).

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
No

Default:

Auto

2.23.20.2.14 Max.-Spatial-Steams

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that enables the use of spatial multiplexing, a technique that increases transmission rates. This involves the parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

The default setting allows settings for the spatial streams to be made automatically to make optimal use of the radio system.

You also have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
One
Two

Default:

Auto

2.23.20.2.15 Send-Aggregates

The settings for frame aggregation are located here. Frame aggregation is an official standard and, according to the 802.11n standard, it is intended to be vendor-independent. It is comparable to the long-existing burst mode.

With frame aggregation for WLAN, the frame is enlarged so that multiple Ethernet packets fit into it. This method shortens the waiting time between data packets and increases throughput. The overhead is reduced to release capacity for transmitting data.

However, the increasing length of the frames increases the likelihood that radio interference will make it necessary to retransmit packets. Furthermore, other stations must wait longer for a channel to become available, and they have to collect several data packets for transmission all at once. By default, frame aggregation is activated. This makes sense if you want to increase the throughput for this station and others on this medium are not important.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.2.16 Min.-HT-MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
MCS 0/8
MCS 1/9
MCS 2/10
MCS 3/11
MCS 4/12
MCS 5/13
MCS 6/14
MCS 7/15

Default:

Auto

2.23.20.2.17 Max.-HT-MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
MCS 0/8
MCS 1/9
MCS 2/10
MCS 3/11
MCS 4/12
MCS 5/13
MCS 6/14
MCS 7/15

Default:

Auto

2.23.20.2.18 Min.-Spatial-Steams

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that enables the use of spatial multiplexing, a technique that increases transmission rates. This involves the parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

The default setting allows settings for the spatial streams to be made automatically to make optimal use of the radio system.

You also have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Auto
One
Two

Default:

Auto

2.23.20.2.19 EAPOL-Rate

Set the data rate for EAPOL transmission here.

The value "Like-Data" transmits the EAPOL data at the same rate as payload data.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

Like-Data
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
T-12M
T-18M
T-36M
T-48M
T-72M
T-96M
T-108M

Default:

Like-Data

2.23.20.2.20 Max.-Aggr.-Packet-Count

This parameter defines the maximum number of packets that may be packed into an aggregate. Aggregation in IEEE 802.11n WLAN transmissions combines multiple data packets into one large packet, so reducing the overhead and speeding up the transmission.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

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

Default:

16

2.23.20.2.21 ProbeRsp-Retries

This is the number of hard retries for probe responses, i.e. messages sent from an access point in answer to a probe request from a client.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0 … 15

Default:

3

2.23.20.2.22 Receive-Aggregates

With this setting you allow or prohibit the reception of aggregated (compiled) data packets (frames) on this interface.

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This method serves to reduce the packet overhead, and the data throughput increases.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.2.23 Use-STBC

Here you activate the use of STBC for data transfer per logical network (SSID).

If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

No
If the WLAN chipset does not support STBC.

Yes
If the WLAN chipset supports STBC.

Default:

No

Yes

2.23.20.2.24 Use-LDPC

Here you activate the use of LDPC for data transfer per logical network (SSID).

If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

No

If the WLAN chipset does not support STBC.

Yes

If the WLAN chipset supports STBC.

Default:

No

Yes

2.23.20.2.25 Convert-to-Unicast

This parameter is used to specify which type of data packets sent in a WLAN as a broadcast are automatically converted into unicast by the device.

Console path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0

None

1

DHCP: Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

2

Multicast: In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

3

DHCP and multicast conversion

Default:

1

2.23.20.3 Encryption

Here you can adjust the encryption settings for each logical wireless LAN network (MultiSSID).

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.3.1 Ifc

Opens the WPA/WEP settings for the available logical WLAN networks.

Console path:

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

2.23.20.3.2 Encryption

Activates the encryption for this logical WLAN.

Console path:

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

Possible values:

No
Yes

Default:

Yes

2.23.20.3.3 Default-Key

Selects the WEP key to be used for encrypting packets sent by this logical WLAN.

Key 1 only applies for the current logical WLAN, keys 2 to 4 are valid as group keys for all logical WLANs with the same physical interface.

Console path:

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

Possible values:

1 … 4

Default:

1

2.23.20.3.4 Method

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Please consider that not all wireless cards support all encryption methods.

Console path:

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

Possible values:

802.11i-WPA-PSK
WEP-128-Bits
WEP-104-Bits
WEP-40-Bits
802.11i-WPA-802.1X
WEP-128-Bits-802.1X
WEP-104-Bits-802.1X
WEP-40-Bits-802.1X
Enhanced-Open
Enhanced-Open-Transitional

Default:

802.11i-WPA-PSK

2.23.20.3.5 Authentication

The encryption method can be selected when using WEP.

For reasons of security we recommend that you use the open system authentication procedure.

Console path:

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

Possible values:

Open-System

For the Open System authentication procedure, all clients are accepted. There is no authentication. The WLAN clients must always transmit correctly encrypted data for this to be forwarded by the base station.

Shared-Key

With the shared key authentication procedure, authentication requires that the WLAN client initially responds by returning a correctly encrypted data packet. Only if this succeeds will the encrypted data from the client be accepted and forwarded. However, this method presents an attacker with a data packet in its encrypted and unencrypted form, so providing the basis for an attack on the key itself.

Default:

Open-System

2.23.20.3.6 Key

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "`0x`".

When using 802.1x in AP mode, the name entered here refers to the RADIUS server.

When using 802.1x in client mode and PEAP or TTLS as the client EAP method, the credentials (user:password) are saved here.

The following lengths result for the formats used:

WPA-PSK

8 to 63 ASCII characters

WEP152 (128 bit)

16 ASCII or 32 hex characters

WEP128 (104 bit)

13 ASCII or 26 hex characters

WEP64 (40 bit)

5 ASCII or 10 hex characters

Console path:

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

Possible values:

Max. 63 characters from `[A-F][a-f][0-9]`

Default:

empty

2.23.20.3.9 WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

Console path:

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

Possible values:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default:

WPA2

2.23.20.3.10 Client-EAP-Method

LANCOM wireless routers and access points in WLAN client operating mode can authenticate themselves to another access point using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.

Please note that the selected client EAP method must match the settings of the access point that this access point is attempting to register with.

In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode.

Console path:

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

Possible values:

TLS
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAP
TTLS/MSCHAPv2
TTLS/MD5
PEAP/MSCHAPv2

Default:

TLS

2.23.20.3.11 WPA-Rekeying-Cycle

Defines how often a WPA key handshake will be retried during an existing connection (rekeying)

Console path:

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

Possible values:

0 … 4294967295 Seconds

Default:

0

Special values:

0

Rekeying deactivated

2.23.20.3.12 WPA1-Session-Keytypes

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Console path:

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

Possible values:

TKIP
AES
TKIP/AES

Default:

TKIP

2.23.20.3.14 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, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

Console path:

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

Possible values:

No

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

2.23.20.3.15 PMK-Caching

Here you enable or disable the usage of PMK caching.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.3.16 Pre-Authentication

Enables pre-authentication support for the corresponding WLAN.

In order to be able to use pre-authentication, PMK caching must be enabled.

Console path:

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

Possible values:

No
Yes

Default:

No

2.23.20.3.17 OKC

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

In the PMK caching status under **Status** > **WLAN** > **PMK-Caching** > **Contents**, OKC PMKs can be identified by the authenticator address `ff:ff:ff:ff:ff:n`, where `n` is the assigned profile number (e.g. `0` for "WLAN-1", `1` for "WLAN1-2", etc.).

For OKC to function, *2.23.20.3.17 OKC* on page 733 must be enabled, and *2.23.20.3.20 PMK-IAPP-Secret* on page 734 must not be empty.

Console path:

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

Possible values:

Yes
No

Default:

Yes

2.23.20.3.19 WPA2-Key-Management

You configure the WPA2 key management with these options.

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.

Console path:

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

Possible values:

Fast-Roaming

Enables Fast Roaming via IEEE 802.11r. In this case, *2.23.20.3.20 PMK-IAPP-Secret* on page 734 must not be empty in non-WLC-AP mode to ensure that the PMK/PMK-R0 is distributed to other access points, allowing Opportunistic Key Caching and Fast Transition to function.

SHA256

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

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.

Default:

Standard

2.23.20.3.20 PMK-IAPP-Secret

Networked APs exchange data about associated WLAN clients by means of the IAPP, so ensuring that the WLAN clients can roam securely in controller-less WLAN networks that are managed by the LANCOM LSR.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

In non-WLC-AP mode, a PMK-IAPP-Secret is a prerequisite for *2.23.20.3.17 OKC* on page 733, fast roaming with *2.23.20.3.19 WPA2-Key-Management* on page 734, and *2.23.20.3.30 Fast-Roaming-Over-the-DS* on page 737.

Console path:

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

Possible values:

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

Default:

empty

Special values:

empty

OKC via IAPP is disabled.

2.23.20.3.21 RADIUS profile

If you are operating an authentication method based on the IEEE 802.1X standard, you specify the profile of a RADIUS server here.

Console path:

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

Possible values:

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

Default:

empty

2.23.20.3.22 Enhanced-Open-Groups

The authentication method Enhanced Open uses elliptic curves.

Console path:

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

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

2.23.20.3.26 SAE-Groups

The authentication method SAE (Simultaneous Authentication of Equals) uses elliptic curves. Further information is available from the *Standards for Efficient Cryptography Group*.

Console path:

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

Possible values:

secp256r1
secp384r1
secp521r1
secp192r1
secp224r1

Default:

secp256r1

secp384r1

secp521r1

2.23.20.3.27 WPA2-3-Session-Keytypes

Here you select the methods that users should be offered to generate the WPA session or group keys. The following Advanced Encryption Standard (AES) methods can be offered.

Console path:

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

Possible values:

AES-CCMP-128
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default:

AES-CCMP-128

2.23.20.3.28 WPA 802.1X security level

Setting the 802.1X security level. WPA3 features the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments.

Operating CNSA Suite B cryptography requires the use of certain cipher suites. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP128 is also enforced with “Suite B 128 bits”.

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

Console path:

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

Possible values:

Default
Suite-B 128-bit

Enabled “Suite B 128 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Suite-B 128-bit

Enabled “Suite B 192 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Default:

Default

2.23.20.3.30 Fast-Roaming-Over-the-DS

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

For this feature to function, *2.23.20.3.20 PMK-IAPP-Secret* on page 734 must not be empty.

Console path:

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

Possible values:

Yes
No

Default:

No

2.23.20.3.31 Transition-Termination

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

Console path:

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

Possible values:

Yes
No

Default:

No

2.23.20.4 Group key

This is where you can specify for each physical wireless LAN interface those WEP group keys 2 to 4, that are used there by the logical wireless LAN networks in common.

If 802.1x/EAP is activated, the group encryption keys are used by 802.1x/EAP and are thus no longer available for WEP encryption.

Console path:

Setup > **Interfaces** > **WLAN**

Possible values:

No
Yes

Default:

No

2.23.20.4.1 Ifc

Opens the WEP group keys for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

No
Yes

Default:

No

2.23.20.4.3 Key-2

WEP group key 2.

You can enter the key as an ASCII character string or as a hexadecimal number (with a leading "0x").

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP152 (128 bit)
16 ASCII or 32 hex characters

WEP128 (104 bit)
13 ASCII or 26 hex characters

WEP64 (40 bit)
5 ASCII or 10 hex characters

2.23.20.4.4 Key-3

WEP group key 3.

You can enter the key as an ASCII character string or as a hexadecimal number (with a leading "0x").

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP152 (128 bit)
16 ASCII or 32 hex characters

WEP128 (104 bit)
13 ASCII or 26 hex characters

WEP64 (40 bit)
5 ASCII or 10 hex characters

2.23.20.4.5 Key-4

WEP group key 4.

You can enter the key as an ASCII character string or as a hexadecimal number (with a leading "0x").

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP152 (128 bit)
16 ASCII or 32 hex characters

WEP128 (104 bit)

13 ASCII or 26 hex characters

WEP64 (40 bit)

5 ASCII or 10 hex characters

2.23.20.4.7 Keytype-2

Select the key length to be used for the WEP group encryption key 2.

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP-156 (128 bit)
WEP128 (104 bit)
WEP64 (40 bit)

Default:

WEP64 (40 bit)

2.23.20.4.8 Keytype-3

Select the key length to be used for the WEP group encryption key 3.

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP-156 (128 bit)
WEP128 (104 bit)
WEP64 (40 bit)

Default:

WEP64 (40 bit)

2.23.20.4.9 Keytype-4

Select the key length to be used for the WEP group encryption key 4.

Console path:

Setup > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Possible values:

WEP-156 (128 bit)
WEP128 (104 bit)
WEP64 (40 bit)

Default:

WEP64 (40 bit)

2.23.20.5 Interpoint settings

Here you can specify important parameters for the communication between and the behavior of base stations.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.5.1 Ifc

Opens the settings for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

2.23.20.5.2 Enable

The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

No
The access point only communicates with mobile clients.

Yes
The access point communicates with other access points and with mobile clients.

Exclusive
The access point only communicates with other base stations.

Default:

No

2.23.20.5.9 Isolated mode

Allows or prohibits the transmission of packets between P2P links on the same WLAN interface (compatibility setting for LCOS versions prior to version 2.70).

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

No
Yes

Default:

No

2.23.20.5.10 Channel selection scheme

In the 5 GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme".

Thus it is recommended for the 5GHz band that one central access point should be configured as "Master" and all other point-to-point partners should be configured as "Slave". In the 2.4GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

Master
This access point makes the decisions when selecting a free WLAN channel.

Slave
All other access points will keep searching until they find a transmitting Master.

Default:

Master

2.23.20.5.11 Link-Loss-Timeout

Time in seconds after which a (DFS) slave considers the link to the master to be lost if no beacons have been received.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

0 … 4294967295 Seconds

Default:

10

2.23.20.5.12 Key-Handshake-Role

Specifies whether this party should act as authenticator or supplicant when WPA is being used. In default mode, the authenticator is the master of a link, in auto mode the authenticator is the device with the lower MAC address.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

Default
Auto

Default:

Default

2.23.20.5.13 Local name

For this physical WLAN interface, enter a name which is unique in the WLAN: This name can be used by other WLAN devices to connect this base station over point-to-point.

You can leave this field empty if the device has only one WLAN interface and already has a device name which is unique in the WLAN, or if the other base stations identify this interface by means of the WLAN adapter's MAC address.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.23.20.5.14 Remote-Status-Reporting

This parameter enables the device to inform its P2P partner whether the signal it is receiving has the required signal strength. This parameter is only relevant if you have defined signal thresholds a P2P link.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

No
Yes

Default:

No

2.23.20.5.15 Network name

Enter a unique name for the network where this WLAN interface is located.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:

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

Default:

empty

2.23.20.6 Client modes

If you operate your device in client mode, you can make detailed settings on its behavior here.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.6.1 Ifc

Opens the settings for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

2.23.20.6.3 Connection keepalive

This option ensures that the client station keeps the connection to the access point alive even if the connected devices are not exchanging any data packets. If this option is disabled, the client station is automatically logged off the wireless network if no packets are transferred over the WLAN connection within a specified time.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

No
Yes

Default:

Yes

2.23.20.6.4 Network types

"Network types" specifies whether the station can only register with infrastructure networks or with adhoc networks as well.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

Infrastructure
Adhoc

Default:

Infrastructure

2.23.20.6.5 Scan bands

This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

2.4/5 GHz
2.4 GHz
5 GHz
2.4GHz/5GHz

Default:

2.4/5 GHz

2.23.20.6.6 Preferred BSS

If the client station is to log onto one particular access point only, the MAC address of the WLAN card in this access point can be entered here.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

Max. 16 characters from `[A-F][a-f][0-9]-:.`

Default:

000000000000

2.23.20.6.7 Address adaptation

In client mode, the client station normally replaces the MAC addresses in data packets from the devices connected to it with its own MAC address. The access point at the other end of the connection only ever "sees" the MAC address of the client station, not the MAC address of the computer(s) connected to it.

In some installations it may be desirable for the MAC address of a computer to be transmitted to the access point and not the MAC address of the client station. The option **Address adaptation** prevents the MAC address from being replaced by the client station. Data packets are transferred with their original MAC addresses.

Address adaptation only works when just one computer is connected to the client station.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

No
Yes

Default:

No

2.23.20.6.12 Selection preference

Here you select how this interface is to be used.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

Signal strength

Selects the profile for the WLAN offering the strongest signal. This setting causes the WLAN module in client mode to automatically switch to a different WLAN as soon as it offers a stronger signal.

Profile

Selects the profile for available WLANs in the order that they have been defined (WLAN index, e.g. WLAN-1, WLAN-2, etc.), even if another WLAN offers a stronger signal. In this setting, the WLAN module in client mode automatically switches to a different WLAN as soon as a WLAN with a lower WLAN index is detected (irrespective of signal strengths).

Default:

Signal strength

2.23.20.6.13 Send-Deauth-upon

This parameter specifies the cases in which a device acting as a WLAN client is able to explicitly log-off from the AP.

Console path:

Setup > **Interfaces** > **WLAN** > **Client-Modes**

Possible values:

Deactivation

Log-off on deactivation of the WLAN

Default:

Deactivation

2.23.20.7 Operational

In the operational settings you can set basic parameters for operating your WLAN interface.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.7.1 Ifc

Opens the settings for the physical WLAN interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Operational**

Possible values:

WLAN-1
WLAN-2

2.23.20.7.2 Operating

Switches the physical WLAN interface on or off separately.

Console path:

Setup > **Interfaces** > **WLAN** > **Operational**

Possible values:

Yes
No

Default:

No

2.23.20.7.3 Operation mode

LANCOMDevices are able to operate in various operating modes:

Console path:

Setup > **Interfaces** > **WLAN** > **Operational**

Possible values:

Access point

As a base station (access point), the device makes the link between WLAN clients and the cabled LAN.

Managed AP

As a managed access point, the device searches for a central WLAN Controller from which it can obtain a configuration.

Station

In station (client) mode, the device itself locates the connection to another access point and attempts to register with a wireless network. In this case the device serves to connect a wired device to a base station over a point-to-point link.

Probe

In "Probe" mode, the spectral scan uses the radio module of the access point. The device cannot transmit or receive data in this mode. On startup of the spectral scan, the device automatically switches to "Probe" mode so that this setting need not be configured manually.

Default:

Access point

2.23.20.7.4 Link-LED-Function

When setting up point-to-point connections or operating the device as a WLAN client, the best possible positioning of the antennas is facilitated if the signal strength can be recognized at different positions. The WLAN link LED can be used for displaying the signal quality during the set-up phase. In the corresponding operating mode, the WLAN link LED blinks faster with better reception quality.

Console path:

Setup > **Interfaces** > **WLAN** > **Operational**

Possible values:

Normal

In this operation mode, the LED uses “inverse flashing” in order to display the number of WLAN clients that are logged on to this access point as clients. There is a short pause after the number of flashes for each client. Select this operation mode when you are operating the device in access point mode.

Client-Mode-Strength

In this operation mode, this LED displays the signal strength of the access point with which the device has registered itself as a client. The faster the LED blinks, the better the signal. Select this operation mode only if you are operating the device in client mode.

P2P-1- to P2P-16-Strength

In this operation mode, the LED displays the signal strength of respective P2P partner with which the device forms a P2P path. The faster the LED blinks, the better the signal.

Default:

Normal

2.23.20.7.5 Broken-Link-Detection

When an access point is not connected to the cabled LAN, it is normally unable to fulfill its primary task, namely the authorization of WLAN clients for access to the LAN. The broken-link detection function allows a device's WLAN to be disabled if the connection to the LAN should fail. Clients associated with that access point are then able to login to a different one (even if it has a weaker signal).

Until LCOS version 7.80, broken-link detection always applied to LAN-1, even if the device was equipped with multiple LAN interfaces. Furthermore, deactivation affected all of the WLAN modules in the device. With LCOS version 7.82, broken-link detection could be bound to a specific LAN interface.

This function allows the WLAN modules in a device to be disabled if the allocated LAN interface has no connection to the LAN.

The interface names LAN-1 to LAN-n represent the logical LAN interfaces. To make use of this function, the physical Ethernet ports on the device must be set with the corresponding values LAN-1 to LAN-n.

Broken-link detection can also be used for WLAN devices operating in WLAN client mode. With broken-link detection activated, the WLAN modules of a WLAN client are only activated when a connection exists between the relevant LAN interfaces and the cabled LAN.

Console path:

Setup > **Interfaces** > **WLAN** > **Operational**

Possible values:

No

Broken-link detection is disabled.

LAN-1 to LAN-n (depending on the LAN interfaces available in the device)

All of the WLAN modules in the device will be deactivated if the LAN interface set here should lose its connection to the cabled LAN.

Default:

No

2.23.20.8 Radio settings

Here you can adjust settings that regulate the physical transmission and reception over your WLAN interface.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.8.1 Ifc

Opens the settings for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

2.23.20.8.2 TX power reduction

In contrast to antenna gain, the entry in the field '"x power reduction" causes a static reduction in the power by the value entered, and ignores the other parameters.

The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

0 … 999

Default:

0

2.23.20.8.3 5 GHz mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds in Turbo Mode up to 108 Mbps.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Auto
Normal

This setting is only available for devices that support DFS2 or DFS3.

11an mixed
Greenfield

Default:

Auto

2.23.20.8.4 Maximum distance

The run-time over large distances between transmitter and receiver give rise to increasing delays for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within a given time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay as required by the data packets for wireless communications.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

0 … 65535 Kilometers

Default:

10

2.23.20.8.6 Band

Selecting the frequency band determines whether the wireless LAN adapter operates in the 2.4 GHz or 5 GHz band, which in turn determines the available radio channels.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

2.4 GHz
5 GHz

Default:

2.4 GHz

2.23.20.8.7 Subbands

In the 5 GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Band-1
Band-2
Band-3
Band-1+2
Band-1+3
Band-2+3
Band-1+2+3

Default:

Band-1

2.23.20.8.8 Radio channel

The radio channel selects a portion of the conceivable frequency band for data transfer.

In the 2.4 GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

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

Default:

11

2.23.20.8.9 2.4 GHz mode

In the 2.4 GHz band, there are two different wireless standards: The IEEE 802.11b standard with a transmission speed of up to 11 Mbps and the IEEE 802.11g standard offering up to 54 Mbps. If 2.4 GHz is selected as the operating frequency, the transmission speed can be selected in addition.

The 802.11g/b compatibility mode offers the highest possible speeds and yet also offers the 802.11b standard so that slower clients are not excluded. In this mode, the WLAN card in the access point principally works with the faster standard and falls back on the slower mode should a client of this type log into the WLAN. In the "2Mbit compatible" mode, the access point supports older 802.11b cards with a maximum transmission speed of 2 Mbps.

Please observe that clients supporting only the slower standards may not be able to register with the WLAN if the speeds set here are higher.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Auto
802.11g/b mixed
802.11g/b 2-Mbit compatible
802.11b (11 Mbit)
802.11g (54 Mbit)
802.11g (108 Mbit)

Default:

Auto

2.23.20.8.10 AP density

The more access points there are in a given area, the more the reception areas of the antennae intersect. The setting "Access point density" can be used to reduce the reception sensitivity of the antenna.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Low
Medium
High
Minicell
Microcell
Off

Default:

Low

2.23.20.8.12 Antenna gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band and 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example

AirLancer	Antenna gain	Cable attenuation	Value to be entered
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

The minimum of 6.5 dBm only applies to legacy abg radio modules with G-mode wireless LAN.

The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

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

Default:

3

2.23.20.8.13 Channel list

This field specifies the subset of channels to be used for automatic channel selection or in client mode.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Max. 48 characters from `[0-9],`

Default:

empty

2.23.20.8.14 Background scan

In order to identify other access points within the device's local radio range, the device can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

If a value is entered here, the device searches the frequencies in the active band that are currently not in use in cycles within this interval in order to find available access points.

The background scan function is usually deployed for rogue AP detection for the device in access point mode. This scan interval should correspond to the time span within which rogue access points should be recognized, e.g. 1 hour.

Conversely, for the device in client mode, the background scan function is generally used for improved mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

When the background scan time is "0" the background scanning function is deactivated.

2.23.20.8.15 DFS Rescan Hours

This parameter sets the hours (0-24) at which the device deletes the DFS database and performs a DFS rescan. The cron command options can be used to define the hour: For example, `1,6,13` to force a DFS rescan at 01:00h, 06:00h or 13:00h, or `0-23/4` for a DFS scan between 0:00h and 23:00h every 4 hours.

During the DFS rescan, the AP scans for as long as it takes to find the configured minimum number of free channels. You define the minimum number of free channels via the parameter *2.23.20.8.27 DFS-Rescan-Num-Channels* on page 760. The device does not perform a DFS rescan If there has not yet been a forced change of channel and if at least the minimum number of free channels were found during the last DFS scan.

The termination of a DFS scan requires that the device is set with the correct system time.

In some countries, the use of the DFS method for automatic channel selection is a legal requirement. With the DFS method (Dynamic Frequency Selection) an AP automatically selects an unused frequency, for example, to avoid interference from radar systems or to distribute WLAN devices as evenly as possible over the entire frequency band. When booting, the device randomly selects a channel from those available (based on the regional settings, for example). The device then checks whether there is a radar signal or another WLAN already on this channel. This scan procedure is repeated until a sufficient number of channels has been found that are free of radar signals and with the lowest possible number of other networks. The device then selects one of the free channels and observes it for 60 seconds to be sure there are no radar signals. For this reason, data traffic may be interrupted for a period of 60 seconds while the frequencies are scanned for a free channel.

By specifying certain times for the DFS rescan you reduce the chance of the 60-second scan occurring at an inappropriate time.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

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

Special values:

empty

The device only performs a DFS rescan when no further free channel is available. This is the case when the number of channels determined during the initial DFS scan falls below the minimum number of free channels.

Default:

empty

2.23.20.8.17 Antenna mask

Antenna grouping can be configured in order to optimize the gain from spacial multiplexing. By default the system automatically selects the optimum grouping setting to match current conditions. You also have the possibility to set an antenna group with a user-defined combination of antennas. The setting has an affect on radiation and reception behavior of the radio system.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Auto
Antenna-1
Antenna-1+2
Antenna-1+3
Antenna-1+2+3
Off

Default:

Auto

2.23.20.8.18 Background-Scan-Unit

Unit for the definition of the background scan interval

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Seconds
Minutes
Hours
Days

Default:

Seconds

2.23.20.8.19 Channel pairing

This value sets the channel pairs used by 11n devices in 40-MHz mode.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

11n-compliant
The device uses the channels as specified by 802.11n. Compared to the former proprietary channels used in Turbo Mode, the 40-MHz channels have shifted by 20 MHz.

legacy-turbo-friendly
Only useful in outdoor environments to avoid overlapping with other 11a paths in turbo mode.

Hours
Days

Default:

11n-compliant

2.23.20.8.20 Preferred DFS scheme

In order to operate the WLAN device in accordance with current ETSI radio standards, select the corresponding standard here.

When upgrading a LCOS version to a current radio standard, the previous setting is retained.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio settings** > **Preferred DFS scheme**

Possible values:

EN 301 893-V1.3
EN 301 893-V1.5
EN 301 893-V1.6
EN 301 893-V1.7

Default:

EN 301 893-V1.7

2.23.20.8.21 CAC duration

Duration of the channel availability check. With this setting you specify how long (in seconds) a WLAN module operating DFS carries out the initial check of the channels before it selects a radio channel and starts with the data transfer.

The duration of the channel availability check is regulated by the appropriate standards (e.g. in Europe by the ETSI EN 301 893). Please observe the regulations valid for your country.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

0 … 4294967295

Default:

60

2.23.20.8.22 Force-40MHz

Always use a 40 MHz wide channel at 2.4 GHz.

Note that this may not be allowed due to corresponding regulations!

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

No
Yes

Default:

No

2.23.20.8.23 Adaptive-Noise-Immunity

A wireless LAN can be subjected to interference from various sources. Devices such as microwave ovens or cordless phones interfere with data transmission, and even the network devices themselves can emit interference and hinder communications. Each type of interference has its own characteristics. Adaptive Noise Immunity (ANI) enables the access point to use various error conditions to determine the best way to compensate for the interference. By automatically increasing noise immunity, the size of the radio cell can be reduced to mitigate the impact of interference on the data transfer.

The current values and any previous actions are to be found under **Status** > **WLAN** > **Noise-Immunity**.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

No
Yes

Default:

Yes

2.23.20.8.24 Max.-Channel-Bandwidth

Specify the maximum frequency range in which the physical WLAN interface is able to modulate the data to be transmitted onto the carrier signals (channel bandwidth).

In the setting **Auto**, the AP automatically adjusts the channel bandwidth to the optimum. You have also the option to disable the automation and deliberately limit the bandwidth. The available values depend on the WLAN standards supported by the device.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Auto

The AP automatically adjusts the channel bandwidth to the optimum. The AP allows the use of the maximum available bandwidth, assuming that the current operating conditions allow this. Otherwise, the AP limits channel bandwidth to 20MHz.

20MHz

The AP uses channels bundled at 20 MHz.

40MHz

The AP uses channels bundled at 40MHz.

80MHz

The AP uses channels bundled at 80MHz.

Default:

Auto

2.23.20.8.25 Allow-PHY-Restarts

With this parameter, you specify whether the device allows PHY restarts in order to receive processable information despite overlapping signals.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

No

This setting prohibits PHY restarts. The WLAN module discards the overlapping data packets and requests retransmission.

Yes

This setting allows PHY restarts. If two WLAN packets are received at the same time (overlap), the WLAN module processes the one with the stronger signal.

Default:

Yes

2.23.20.8.26 DFS-Rescan-Flush-Clear-Channels

With this parameter you specify whether, after a DFS rescan was completed, the physical WLAN interface deletes occupied channels or saves them for subsequent DFS rescans.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Yes

The physical WLAN interface deletes occupied channels after completing a DFS rescan so that they are available again for a new DFS rescan.

No

The device saves occupied channels after completing a DFS rescan and so that the device immediately skips them during a new DFS rescan.

Default:

No

2.23.20.8.27 DFS-Rescan-Num-Channels

This parameter specifies the minimum number of free channels that a DFS scan is required to find.

With the default value of 2 the AP continues to run a DFS scan until 2 free channels are available. If the AP recognizes an active radar pattern during subsequent operations, at least one other free channel is available for the AP to switch to directly.

If a high number of channels is specified, the initial DFS scan has to examine a large number of channels. Scanning takes 60 seconds per channel. In this context please observe the information given under *2.23.20.8.15 DFS Rescan Hours* on page 755.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

0 … 4294967295

Special values:

0

This value disables the limit. The physical WLAN interface performs a DFS scan on all available channels.

Default:

2

2.23.20.8.28 Preferred 2.4 scheme

This parameter sets the version of the EN 300 328 standard operated by the device in the 2.4 GHz band.

Should you carry out a firmware update, the current version is retained. New devices and devices subject to a configuration reset operate version 1.8 by default.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

EN300328-V1.7
EN300328-V1.8

Default:

EN300328-V1.8

2.23.20.8.29 Indoor-Only-Operation

If indoor-only operation is activated, the 5 GHz-band channels are limited to the 5.15 - 5.25 GHz spectrum (channels 36-48) in ETSI countries. Radar detection (DFS) is switched off and the mandatory interruption after 24 hours is no longer in effect. This mode reduces the risk of interruption due to false radar detections. In the 2.4 GHz band in France, the channels 8 to 13 are also permitted, meaning that more channels are available.

Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Yes
No

Default:

No

2.23.20.8.33 Power-Setting

In versions before LCOS 10.30, the current WLAN transmission power could be reduced by a fixed, configured value. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5 GHz subbands. For example, higher transmission powers are permitted in the 5 GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. As of LCOS 10.30, the actual maximum transmission power can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

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

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Automatic

The maximum permitted transmission power that can be realized by the hardware of the access point is used.

Manual

The desired transmission power is to be set in dBm in the EIRP field.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically. The actual value can be checked in LANmonitor or on the CLI by means of the command `show wlan`.

Default:

Automatic

2.23.20.8.34 EIRP

With the setting for WLAN transmission power in 2.23.20.8.33 is set to manual, the value set here is taken in dBm.

Console path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

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

2.23.20.8.35 Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the

retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

Console path:

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

Possible values:

0 … 20

2.23.20.9 Services

Here you can set the parameters that influence the performance of your WLAN interface.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.9.1 Ifc

Opens the settings for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Performance**

2.23.20.9.2 Tx bursting

Enables/prevents packet bursting for increasing throughput. Bursting leads to less fairness on the medium.

Console path:

Setup > **Interfaces** > **WLAN** > **Performance**

Possible values:

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

Default:

0

2.23.20.9.4 Fast frames

This entry contains the status values for Fast frames.

Console path:

Setup > **Interfaces** > **WLAN** > **Performance**

2.23.20.9.5 QoS

With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

Console path:

Setup > **Interfaces** > **WLAN** > **Performance**

Possible values:

No
Yes

Default:

No

2.23.20.9.6 Airtime-Fairness-Mode

Airtime Fairness is a feature that shares the available bandwidth fairly between all of the active clients. Especially useful in high-density environments, it results in an improvement to WLAN performance. **Airtime Fairness** is activated by default.

Console path:

Setup > **Interfaces** > **WLAN** > **Performance**

Possible values:

Round-Robin
Each client in turn receives a time slot for transmission.

Equal-Airtime
All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because the access point can send more data to the client in the same amount of time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

Pref.-11n-Airtime
This setting prefers clients that use IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent much faster to clients using IEEE 802.11n.

Equal-Volume
This setting distributes the airtime between the clients to ensure that all clients receive the same amount of throughput by the access point. However, slower clients will slow down all clients.

This setting is only recommended when it is necessary for all clients to receive the same throughput.

Default:

Equal-Airtime

2.23.20.10 Beaconing

Roaming settings are only relevant in the base-station operating mode. The wireless LAN access point (WLAN AP) periodically transmits a radio signal (beacon) so that the clients can detect it or the logical wireless networks (SSIDs) that it provides.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.10.1 Ifc

Opens the Expert settings for the available physical interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Beaconing**

2.23.20.10.2 Beacon period

This value defines the time interval in K s between beacon transmission (1 K s corresponds to 1024 microseconds and is a measurement unit of the 802.11 standard. 1 K s is also known as a Timer Unit (TU)). Smaller values result in a shorter beacon timeout period for the client and enable quicker roaming in case of failure of an access point, but they also increase the WLAN overhead.

Console path:

Setup > **Interfaces** > **WLAN** > **Beaconing**

Possible values:

20 … 65535 Timer unit

Default:

100

2.23.20.10.3 DTIM period

This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

Console path:

Setup > **Interfaces** > **WLAN** > **Beaconing**

Possible values:

1 … 255

Default:

1

2.23.20.10.4 Beacon order

Beacon order refers to the order in which beacons are sent to the various WLAN networks. For example, if three logical WLAN networks are active and the beacon period is 100 K s, then the beacons will be sent to the three WLANs every 100 K s. Depending on the beacon order, the beacons are transmitted at times as follows.

Some older WLANs are unable to process the quick succession of beacons which occur with simple burst. Consequently these clients often recognize the first beacons only and can only associate with this network. Staggered transmission of beacons produces better results but increases load on the access point's processor. Cyclic transmission proves to be a good compromise as all networks are transmitted first in turn.

Console path:

Setup > **Interfaces** > **WLAN** > **Beaconing**

Possible values:

Cyclic

In this mode the access point transmits the first beacon transmission at 0 K s to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 K s) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 K s) the order is WLAN-3, WLAN-1, WLAN-2. After this the sequence starts again.

Staggered

In this mode, the beacons are not sent together at a particular time, rather they are divided across the available beacon periods. Beginning at 0 K s, WLAN-1 only is sent; after 33.3 K s WLAN-2, after 66.6 K s WLAN-3. At the start of a new beacon period, transmission starts again with WLAN-1.

Simple burst

In this mode the access point always transmits the beacons for the WLAN networks in the same order. The first beacon transmission (0 K s) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

Default:

Cyclic

2.23.20.11 Roaming

Roaming settings are only relevant in the client operating mode. They regulate the way that the client switches between multiple base stations, where available.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.11.1 Ifc

Opens the Expert settings for the available physical interfaces.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.11.2 Beacon-Miss-Threshold

The beacon loss threshold defines how many access-point beacons can be missed before a registered client starts searching again.

Higher values will delay the recognition of an interrupted connection, so a longer time period will pass before the connection is re-established.

The lower the value set here, the sooner a potential interruption to the connection will be recognized; the client can start searching for an alternative access point sooner.

Values which are too small may cause the client to detect lost connections more often than necessary.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

4

2.23.20.11.3 Roaming threshold

This value is the percentage difference in signal strength between access points above which the client will switch to the stronger access point.

Other contexts require the value of signal strengths in dB. The following conversion applies:

Decibel	Percent
64dB	100%
32dB	50%
0dB	0%

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

15

2.23.20.11.4 No roaming threshold

This threshold refers to the field strength in percent. Field strengths exceeding the value set here are considered to be so good that no switching to another access point will take place.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

45

2.23.20.11.5 Force roaming threshold

This threshold refers to the field strength in percent. Field strengths below the value set here are considered to be so poor that a switch to another access point is required.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

12

2.23.20.11.6 Soft roaming

This option enables a client to use scan information to roam to a stronger access point (soft roaming). Roaming due to connection loss (hard roaming) is unaffected by this. The roaming threshold values only take effect when soft roaming is activated.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

No
Yes

Default:

Yes

2.23.20.11.7 Connect threshold

This value defines field strength in percent defining the minimum that an access point has to show for a client to attempt to associate with it.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

0

2.23.20.11.8 Connect hold threshold:

This threshold defines field strength in percent. A connection to an access point with field strength below this value is considered as lost.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 99 Percent (%)

Default:

0

2.23.20.11.9 Min-Connect-Signal-Level

Similar to the connection threshold, but specified as absolute signal strength.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … -128 dBm

Default:

0

2.23.20.11.10 Min-Connect-Hold-Signal-Level

Similar to the connection hold threshold, but specified as absolute signal strength.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … -128 dBm

Default:

0

2.23.20.11.11 Block time

If your device is operating as a WLAN client in an environment with multiple WLAN access points all with the same SSID, you can define a time period during which the WLAN client will avoid associating with a particular access point after receiving an "association-reject" from it.

Console path:

Setup > **Interfaces** > **WLAN** > **Roaming**

Possible values:

0 … 4294967295 Seconds

Default:

0

2.23.20.12 Interpoint peers

Here you enter the wireless base stations that are to be networked via the point-to-point connection.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.12.1 Ifc

Here you select the wireless base stations that are to be networked via the point-to-point connection.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

2.23.20.12.2 Recognize-By

Here you select the characteristics to be used to identify the P2P peer.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

MAC address

Select this option if the devices are to recognize P2P partners by their MAC address. In this case, fill-out the "MAC address" with the WLAN MAC address of the physical WLAN interface of the P2P partner.

Host name

Select this option if the devices are to recognize P2P partners by their peer name. In this case, fill-out the "Peer name" with the device name of the P2P peer or, alternatively, the "Peer name" defined in the physical settings.

Serial-Autoconfig

Use this setting if the P2P peers are to exchange their MAC addresses via a serial connection.

Default:

MAC address

2.23.20.12.3 MAC address

MAC address of the P2P peer.

If you work with detection by MAC address, enter the MAC address of the WLAN adapter here and not that of the device itself.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

Max. 12 characters from `[A-Z][a-z][0-9]-:`

Default:

empty

2.23.20.12.4 Peer-Name

Station name of the P2P remote station

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.23.20.12.5 Operating

Activates or deactivates this point-to-point channel.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

No
Yes

Default:

No

2.23.20.12.6 Tx-Limit

With this setting you limit the bandwidth of the uplink (in kbps) for the configured point-to-point link.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

This value 0 disables the limit (= unlimited bandwidth).

2.23.20.12.7 Rx-Limit

With this setting you limit the bandwidth of the downlink (in kbps) for the configured point-to-point link.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

This value 0 disables the limit (= unlimited bandwidth).

2.23.20.12.8 Key value

Specify the WPA2 passphrase for the P2P connection. Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

min. 8 characters; max. 63 characters from

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

2.23.20.12.9 Connect threshold

A WLAN interface can manage point-to-point links to more than one remote station, and each of these connections can have a different "nominal" signal strength.

Connect threshold

The value specifies the beacon signal strength with which the remote site must be received in order to establish the point-to-point link.

Connect hold threshold

The value specifies the beacon signal strength with which the remote site must be received in order to keep the point-to-point link.

Both values represent the necessary signal-to-noise ratio (SNR) in percentage. The purpose of the two different values is to establish a hysteresis which avoids connection state flatter. Fast connection state changes would otherwise lead to instability, for example, in the topology decisions of the spanning-tree algorithm.

The **Connect-Hold-Threshold** must be lower than the **Connect-Threshold**.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

0 … 255

Default:

0

Special values:

0

The value 0 disables the corresponding limits.

2.23.20.12.10 Connect hold threshold

A WLAN interface can manage point-to-point links to more than one remote station, and each of these connections can have a different "nominal" signal strength.

Connect threshold

The value specifies the beacon signal strength with which the remote site must be received in order to establish the point-to-point link.

Connect hold threshold

The value specifies the beacon signal strength with which the remote site must be received in order to keep the point-to-point link.

Both values represent the necessary signal-to-noise ratio (SNR) in percentage. The purpose of the two different values is to establish a hysteresis which avoids connection state flatter. Fast connection state changes would otherwise lead to instability, for example, in the topology decisions of the spanning-tree algorithm.

The **Connect-Hold-Threshold** must be lower than the **Connect-Threshold**.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Peers**

Possible values:

0 … 255

Default:

0

Special values:

0

The value `0` disables the corresponding limits.

2.23.20.13 Network-Alarm-Limits

This table contains the settings for the network alarm limits for the device's logical WLAN networks (SSIDs).

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.13.1 Ifc

From the SSIDs available on the device (e.g. WLAN-1, WLAN-1-2), select the logical WLAN network (SSID) for which you want to edit the network alarm limits.

Console path:

Setup > **Interfaces** > **WLAN** > **Network-Alarm-Limits**

2.23.20.13.2 Phy-Signal

The negative threshold value for the signal level of the corresponding SSID. If the value falls below this threshold, an alert is issued.

Console path:

Setup > **Interfaces** > **WLAN** > **Network-Alarm-Limits**

Possible values:

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

Default:

0

Special values:

0

This value disables the checking.

2.23.20.13.3 Total retries

The threshold value for the total number of transmission retries for the corresponding SSID, per mille. Once the value is reached, an alert is issued.

Console path:

Setup > **Interfaces** > **WLAN** > **Network-Alarm-Limits**

Possible values:

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

Default:

0

Special values:

0

This value disables the checking.

2.23.20.13.4 Tx-Errors

The total number of lost packets for the corresponding SSID, per mille. Once the value is reached, an alert is issued.

Console path:

Setup > **Interfaces** > **WLAN** > **Network-Alarm-Limits**

Possible values:

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

Default:

0

Special values:

0

This value disables the checking.

2.23.20.14 Interpoint-Alarm-Limits

This table contains the settings for the interpoint alarm limits for the device's P2P connections (SSIDs).

SNMP ID: 2.23.20.14

Telnet path: /Setup/Interfaces/WLAN

2.23.20.14.1 Ifc

Select the P2P connection here for which you wish to set the interpoint alarm limits.

SNMP ID: 2.23.20.14.1

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

› Choose from the P2P connections available in the device, e.g. P2P-1, P2P-2, etc.

2.23.20.14.2 Phy-Signal

The negative threshold value for the signal level of the corresponding P2P connection. If the value falls below this threshold, an alert is issued. Setting this value to 0 deactivates the check.

SNMP ID: 2.23.20.14.2

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

› 3 numerical characters

Default: 0

2.23.20.14.3 Total-Retries

The threshold value for the total number of transmission retries for the corresponding P2P connection. Once the value is reached, an alert is issued. Setting this value to 0 deactivates the check.

SNMP ID: 2.23.20.14.3

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

› 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.14.4 Tx-Errors

The total number of lost packets for the corresponding P2P connection. Once the value is reached, an alert is issued. Setting this value to 0 deactivates the check.

SNMP ID: 2.23.20.14.4

Telnet path: /Setup/Interfaces/WLAN/Interpoint-Alarm-Limits

Possible values:

› 4 numeric characters to specify the repetitions in per mille

Default: 0 per mille

2.23.20.15 Probe settings

This table contains the settings for the spectral scan.

The device cannot transmit or receive data in this mode.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.15.1 Ifc

Opens the settings for the available physical WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

2.23.20.15.2 Radio bands

Here you can select which frequency bands should be analyzed by spectral scanning.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

2.4GHz
5GHz
2.4GHz/5GHz

Default:

2.4GHz

2.23.20.15.3 Subbands-2.4GHz

This setting specifies which subbands of the 2.4GHz frequency are to be analyzed.

The spectral scan only takes this field into account when either '2.4GHz' or '2.4GHz/5GHz' is set in **Radio bands**.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

Band-1
Band-2
Band-1+2

Default:

Band-1

2.23.20.15.4 Channel-List-2.4GHz

Specify in this field the channel list for the spectral scan in the 2.4GHz frequency band. Individual channels are separated with commas.

There is no need to change the default values of the spectral scan for its operation. The spectral scan examines the frequency bands in 20MHz-wide blocks at a time. Due to the 5MHz gaps between the individual 20MHz-wide channels in the 2.4GHz radio band, the channels specified result in a continuous scan of the entire 2.4GHz radio band. In the 5GHz band, the channel bandwidth is also 20MHz, and the individual channels lie next to each other with no overlapping. When no channels are specified, all channels are scanned which results in a complete scan in the 5GHz band.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

1,5,9,13

2.23.20.15.5 Subbands-5GHz

This setting specifies which subbands of the 5GHz frequency are to be analyzed.

The spectral scan only takes this field into account when either "5GHz" or "2.4GHz/5GHz" is set in **Radio bands**.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

Band-1
Band-2
Band-1+2

Default:

Band-1

2.23.20.15.6 Channel-List-5GHz

In this field, specify the list of channels for the spectral scan in the 5GHz frequency band. Individual channels are separated with commas.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.23.20.15.7 Channel-Dwell-Time

Determine here the number of milliseconds the spectral scan dwells on a channel.

The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached. The default value is generally adequate. Only lower the value when you need a more accurate resolution, and when the performance of your browser and PC is high enough to process the faster display of the readings.

Console path:

Setup > **Interfaces** > **WLAN** > **Probe-Settings**

Possible values:

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

Default:

250

2.23.20.16 IEEE802.11u

Determine here the number of milliseconds the spectral scan dwells on a channel.

The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached. The default value is generally adequate. Only lower the value when you need a more accurate resolution, and when the performance of your browser and PC is high enough to process the faster display of the readings.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.16.1 Ifc

Name of the logical WLAN interface that you are currently editing.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

2.23.20.16.2 Operating

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

No
Yes

Default:

No

2.23.20.16.3 Hotspot2.0

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

No
Yes

Default:

No

2.23.20.16.4 Internet

Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

No
Yes

Default:

No

2.23.20.16.5 Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

Private

Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.

Private-GuestAcc

Similar to `Private`, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

Public-Charge

Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.

Public-Free

Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.

Personal-Dev

In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.

Emergency

Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

Experimental

Describes networks that are set up for testing purposes or are still in the setup stage.

Wildcard

Placeholder for previously undefined network types.

Default:

Private

2.23.20.16.6 Asra

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

No
Yes

Default:

No

2.23.20.16.7 HESSID

Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point (its BSSID) serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT".

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

BSSID
user
None

Default:

BSSID

2.23.20.16.8 HESSID-MAC

If you selected the setting `user` for the **HESSID**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address.

Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., `008041AEFD7E` for the MAC address `00:80:41:ae:fd:7e`.

If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

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

Default:

000000000000

2.23.20.16.10 ANQP profile

This parameter is used to specify a valid ANQP profile.

Enter a name from the table **Setup** > **IEEE802.11u** > **ANQP-Profile**.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

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

Default:

empty

2.23.20.16.13 HS20-Profile

This parameter is used to specify a valid Hotspot-2.0 or HS20 profile.

Enter a name from the table **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**.

Console path:

Setup > **Interfaces** > **WLAN** > **IEEE802.11u**

Possible values:

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

Default:

empty

2.23.20.19 Interpoint-transmission

This table contains the transmission settings for the individual P2P links.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.19.1 Ifc

Name of the logical P2P interface which you selected.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Select from the available P2P links.

2.23.20.19.2 Packet size

Select the maximum size of data packets on a P2P link.

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

600 … 2347

Default:

1600

2.23.20.19.3 Min-Tx-Rate

Specify the minimum transmission rate in Mbps in the direction of transmission.

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients (Auto). The access point adjusts the transmission speeds to the reception conditions. You also have the option of preventing dynamic speed adjustment by entering a fixed transmission speed.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

2.23.20.19.6 RTS-Threshold

Use this field to define the RTS threshold. If the size of the packets for transmission exceeds this value, the device uses the RTS/CTS protocol in order to prevent the increased probability of collisions and the associated "hidden station" phenomena.

Since the RTS packets are generally very short and the use of RTS/CTS increases the overhead, using this method only pays off if you are using longer data packets where collisions are likely. The best value can be found using trial and error tests on location.

The RTS threshold value also has to be set in the interpoint peer, as far as the driver and/or operating system allow this.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

60 … 2347

Default:

2347

2.23.20.19.7 11b-Preamble

Specify whether your device uses a long preamble in 802.11b mode.

Normally every WLAN client (in this case the P2P slave) independently negotiates the necessary length of the preamble for communication with the base station (in this case the P2P master). However, in some rare cases it is necessary to ignore this handshake process and use the long WLAN preamble, although this is less advantageous.

Only enable the long WLAN preamble if it precisely resolves your wireless problems.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto

The P2P slave automatically negotiates the length of the preamble (short/long) required to communicate with the P2P-master.

Long

The P2P slave does not negotiate and always uses a long preamble.

Default:

Auto

2.23.20.19.9 Max-Tx-Rate

Specify the maximum transmission rate in Mbps in the direction of transmission.

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients (Auto). The access point adjusts the transmission speeds to the reception conditions. You also have the option of preventing dynamic speed adjustment by entering a fixed transmission speed.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

2.23.20.19.10 Min.-Frag.-Length

Using this input field you define the minimum length of packet fragments, below which the device rejects data packet fragments.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

0 … 65535

Special values:

0, 1

The device allows for packet fragments of any length.

Default:

16

2.23.20.19.11 Soft-Retries

Enter the number of transmission attempts that the device tries if the hardware cannot send a data packet. The total number of transmission attempts results from the calculation `(Soft-Retries + 1) * Hard-Retries`.

The advantage of using soft retries at the expense of hard retries is that the rate-adaption algorithm immediately begins the next series of hard retries with a lower data rate.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

0 … 255

Default:

10

2.23.20.19.12 Hard-Retries

Enter the number of transmission attempts that the device attempts before the hardware reports a Tx error. The smaller the value you choose, the shorter is the time that an unsendable packet will block the transmitter. If the hardware cannot send a data packet, you have the option to continue the attempts on the software side. For more information, see the parameter **Soft-Retries**.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

0 … 255

Default:

10

2.23.20.19.13 Short guard interval

Enable or disable the short guard interval.

Put simply, the guard interval reduces the signal distortion caused by intersymbol interference (ISI) when using signal multiplexing (OFDM). The option reduces the transmission pause between two signals from 0.8 s (default) to 0.4 s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto

The device activates the short guard interval in automatic mode, provided that the remote station supports this.

No

Disables the short guard interval.

Default:

Auto

2.23.20.19.14 Max.-Spatial-Steams

Specify the maximum number of allowed spatial streams.

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that the device can use for spatial multiplexing, a

technique that increases transmission rates. This allows parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

With the factory setting, the device sets up the spatial streams automatically to make optimal use of the radio system. Alternatively you have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
One
Two
Three

Default:

Auto

2.23.20.19.15 Send-Aggregates

With this setting you configure the transmission of aggregated data packets. Frame aggregation is an official standard and, according to the 802.11n standard, it is intended to be vendor-independent. It is comparable to the long-existing burst mode.

For frame aggregation, the device combines multiple data packets (frames) to a larger packet—by increasing the length of the WLAN frame—and sends them together. The method shortens the waiting time between data packets and also reduces the overhead, so increasing the data throughput.

However, with increased frame length, the probability increases that the device must resend the packets, for example, due to radio interference. Other stations must also wait for a free channel and collect their data packets until they have multiple packets that they can send at one time.

Frame aggregation is enabled in the factory settings. This option makes sense if you want to increase the throughput for your device and others on this medium are not important. Frame aggregation is not suitable when working with mobile receivers or real-time data transmissions such as voice over IP.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.19.16 Min.-HT-MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the factory settings the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

2.23.20.19.17 Max.-HT-MCS

MCS (Modulation Coding Scheme) automatically adapts transmission speeds. In the 802.11n standard it defines a number of variables that specify the number of spatial streams, the modulation and the data rate of each data stream, among others.

In the factory settings the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You also have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

2.23.20.19.18 Min.-Spatial-Steams

Specify the minimum number of allowed spatial streams.

Spatial streams add a third dimension to the frequency-time matrix available to radio communications: Space. An array of multiple antennas provides the receiver with spatial information that the device can use for spatial multiplexing, a technique that increases transmission rates. This allows parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This leads to a significant increase in the performance of the radio system.

With the factory setting, the device sets up the spatial streams automatically to make optimal use of the radio system. Alternatively you have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Auto
One
Two
Three

Default:

Auto

2.23.20.19.19 EAPOL-Rate

Set the data rate in Mbps for EAPOL transmission.

WLAN clients use EAP over LAN (EAPOL) to login to the access point by WPA and/or 802.1x. They encapsulate EAP packets in Ethernet frames to allow EAP communications on layer-2 connections.

Under certain circumstances it may be desirable to select a lower data rate for the transfer of EAPOL packets than that available for the payload data. For example, in the case of mobile WLAN clients, high data rates can cause the loss of

EAPOL packets, which in turn leads to considerable delays in client association. This procedure can be stabilized by selecting specific data rates for EAPOL.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

Like-Data

In this setting, the device transmits the EAPOL data at the same rate as payload data.

1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
HT-1-6.5M
HT-1-13M
HT-1-19.5M
HT-1-26M
HT-1-39M
HT-1-52M
HT-1-58.5M
HT-1-65M
HT-2-13M
HT-2-26M
HT-2-39M
HT-2-52M
HT-2-78M
HT-2-104M
HT-2-117M
HT-2-130M

Default:

Like-Data

2.23.20.19.20 Max.-Aggr.-Packet-Count

Using this parameter, you define the maximum number of packets the device may combine into one aggregate. Aggregation in IEEE 802.11n WLAN transmissions combines multiple data packets into one large packet, so reducing the overhead and speeding up the transmission.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

0 … 11/16/24 (device dependent)

Special values:

0

The device automatically uses the highest value allowed on the hardware side.

Default:

0

2.23.20.19.22 Receive-Aggregates

With this setting you configure the reception of aggregated data packets. Frame aggregation is an official standard and, according to the 802.11n standard, it is intended to be vendor-independent. It is comparable to the long-existing burst mode.

For frame aggregation, the device combines multiple data packets (frames) to a larger packet—by increasing the length of the WLAN frame—and sends them together. The method shortens the waiting time between data packets and also reduces the overhead, so increasing the data throughput.

However, with increased frame length, the probability increases that the device must resend the packets, for example, due to radio interference. Other stations must also wait for a free channel and collect their data packets until they have multiple packets that they can send at one time.

Frame aggregation is enabled in the factory settings. This option makes sense if you want to increase the throughput for your device and others on this medium are not important. Frame aggregation is not suitable when working with mobile receivers or real-time data transmissions such as voice over IP.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.19.23 Use-STBC

Activate the space time block coding (STBC) here.

STBC is a method for improving the reception conditions. The function additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

If the WLAN chipset does not support STBC, you cannot set this parameter to **Yes**.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.19.24 Use-LDPC

Activate the low density parity check here (LDPC).

LDPC is an error correction method. Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data rate.

If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Transmission**

Possible values:

No
Yes

Default:

Yes

2.23.20.20 Interpoint-Encryption

This table contains the encryption settings of the physical WLAN interface for P2P links.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.20.1 Ifc

Name of the physical WLAN interface

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

2.23.20.20.2 Encryption

Enables or disables the WPA/WEP encryption for P2P connections over the respective interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

No
Yes

Default:

Yes

2.23.20.20.3 Default-Key

WEP keys with which the device encrypts the packets sent over this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

0 … 9

Default:

1

2.23.20.20.4 Method

Selects the encryption method or, for WEP, the key length which the device uses for the encryption of P2P data packets.

Please note that not every client (or their hardware) supports every encryption method.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

802.11i-WPA-PSK
WEP-128-Bit
WEP-104-Bit
WEP-40-Bit

Default:

802.11i-WPA-PSK

2.23.20.20.9 WPA-Version

WPA version that the device offers a client for WPA encryption.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default:

WPA2

2.23.20.20.11 WPA-Rekeying-Cycle

Specify the intervals at which the device repeats the WPA key handshake. This is the time in seconds after which the access point performs an exchange of the keys used when using a WPA version. By default, the value is set to 0, so there is no renegotiation of the key.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables the renegotiation of a new WPA key at the device. Rekeying can still be triggered by the client.

Default:

0

2.23.20.20.12 WPA1-Session-Keytypes

Select the method or methods that the device offers the remote station for generating the WPA session or group key for WPA1. The device can provide the Temporal Key Integrity Protocol (TKIP) method, the Advanced Encryption Standard (AES) method, or both.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

TKIP
AES
TKIP/AES

Default:

TKIP

2.23.20.20.14 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, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

No
The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory
The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional
The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

2.23.20.20.19 WPA2 key management

You can configure the WPA2 key management with these options.

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.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

SHA256

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

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.

Default:

Standard

2.23.20.20.26 SAE-Groups

The authentication method SAE (Simultaneous Authentication of Equals) uses elliptic curves. Further information is available from the *Standards for Efficient Cryptography Group*.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

secp256r1
secp384r1
secp521r1
secp192r1
secp224r1

Default:

secp256r1

secp384r1

secp521r1

2.23.20.20.27 WPA2-3-Session-Keytypes

Here you select the methods that users should be offered to generate the WPA session or group keys. The following Advanced Encryption Standard (AES) methods can be offered.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Encryption**

Possible values:

AES-CCMP-128
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default:

AES-CCMP-128

2.23.20.21 Coexistence settings

This table contains the settings for the parallel operation of multiple WLANs.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.21.1 Ifc

This entry lists all of the interfaces available with the device (such as WLAN-1, WLAN 2).

Console path:

Setup > **Interfaces** > **WLAN** > **Coexistence-Settings**

2.23.20.21.2 Coexistence

Use this entry to specify whether multiple WLAN interfaces are permitted to operate in parallel.

Console path:

Setup > **Interfaces** > **WLAN** > **Coexistence-Settings**

Possible values:

No
Yes

Default:

Yes

2.23.20.21.3 Min.-Ignore-Prio

.

Console path:

Setup > **Interfaces** > **WLAN** > **Coexistence-Settings**

Possible values:

None
Beacon
Voice

2.23.20.22 Interpoint-Rate-Selection

In this directory, you configure the data rates for communications between the base stations for each P2P link.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.22.1 1M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx-required

2.23.20.22.2 2M

Here you configure how the AP is to handle this data rate for this P2P link.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx-required

2.23.20.22.3 Ifc

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

2.23.20.22.4 5.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.6 11M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.8 6M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.9 9M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.10 12M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.11 18M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.12 24M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.13 36M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.14 48M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.15 54M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.28 HT-1-6.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.29 HT-1-13M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.30 HT-1-19.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.31 HT-1-26M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.32 HT-1-39M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.33 HT-1-52M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.34 HT-1-58.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.35 HT-1-65M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.36 HT-2-13M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.37 HT-2-26M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.38 HT-2-39M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.39 HT-2-52M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.40 HT-2-78M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.41 HT-2-104M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is “supported” and “required”, but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.42 HT-2-117M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is "supported", but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.43 HT-2-130M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the other base stations that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the other base stations. If the base station does not support a particular rate, the AP will reject the corresponding connection request.

Rx/Tx

The AP announces to the other base stations that the rate is "supported". The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx-required

The AP announces to the other base stations that the rate is "supported" and "required", but does not use the rate to communicate with the other base stations.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.44 HT-3-19.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.45 HT-3-39M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.46 HT-3-38.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.47 HT-3-78M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.48 HT-3-117M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.49 HT-3-156M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.50 HT-3-175.5M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.22.51 HT-3-195M

This entry shows which P2P link is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Interpoint-Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with other base stations.

Rx/Tx

The AP announces to the other base stations that the rate is “supported”. The AP also uses the rate to communicate with the other base stations. However, the AP also accepts requests from base stations that do not support this rate.

Rx

The AP announces to the other base stations that the rate is “supported”, but does not use the rate to communicate with the other base stations.

Default:

Rx/Tx

2.23.20.23 Adaptive-RF-Optimization

Adaptive RF Optimization constantly monitors the WLAN environment and evaluates the quality of the network based on the “Wireless Quality Indicators”. If the quality drops, the Adaptive RF Optimization triggers a change to a better suited channel.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.23.1 Ifc

Shows the interface for the Adaptive RF Optimization.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

2.23.20.23.2 Operating

Activates or deactivates Adaptive RF Optimization for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

No
Yes

Default:

No

2.23.20.23.3 Min-Client-Phy-Signal

Setting for the minimum signal strength of clients.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

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

Default:

15

2.23.20.23.4 Min-Client-Tx-Packets

Setting for the minimum number of packets sent to a client.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

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

Default:

30

2.23.20.23.5 Tx-Client-Retry-Ratio-Limit

In this field you specify how quickly a packet is resent to a client.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

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

Default:

70

2.23.20.23.6 Noise-Limit

Setting for the upper limit of acceptable noise on the channel.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

-70

2.23.20.23.7 Marked-Channel-Timeout

When a channel is considered unusable it is marked/blocked for the time specified here.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

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

Default:

20

2.23.20.23.8 Trigger-Timespan

The trigger timespan set here determines how long a limit is continuously exceeded before an action is triggered.

Console path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1

2.23.20.24 Redundancy settings

In this directory, you configure the dynamic adjustment of transmission power in the event of the failure of an AP a cluster of several APs.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.24.1 Ifc

The interface that this entry refers to.

Console path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

2.23.20.24.2 Other APs expected

Use this item to specify the number of other APs that are located in the AP cluster.

So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs is equal to the number of expected devices. The other APs return their transmission power to the default value.

Console path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

Possible values:

Max. 5 characters from `[0-9]`

2.23.20.24.3 Backup transmission power reduction

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

Console path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

Possible values:

Max. 3 characters from `[0-9]`

2.23.20.25 Rate selection

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates "announced" by the AP to the client for its communication with the AP (RX).

This rate adaptation specifies a minimum and a maximum data rate, and it also allows certain data rates between these limits to be disabled. This can save airtime under certain circumstances.

The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

In this directory you configure these data rates.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.25.1 1M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

2.23.20.25.2 2M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

2.23.20.25.3 Ifc

This entry shows which interface is being configured.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

2.23.20.25.4 5.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.6 11M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.8 6M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.9 9M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.10 12M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.11 18M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.12 24M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.13 36M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.14 48M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.15 54M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.28 HT-1-6.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.29 HT-1-13M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.30 HT-1-19.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.31 HT-1-26M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.32 HT-1-39M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.33 HT-1-52M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.34 HT-1-58.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.35 HT-1-65M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.36 HT-2-13M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.37 HT-2-26M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.38 HT-2-39M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.39 HT-2-52M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.40 HT-2-78M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.41 HT-2-104M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.142 HT-2-117M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.43 HT-2-130M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.44 HT-3-19.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.45 HT-3-39M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.46 HT-3-58.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.47 HT-3-78M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.48 HT-3-117M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.49 HT-3-156M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.50 HT-3-175.5M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.25.51 HT-3-195M

Here you configure how the AP is to handle this data rate for this interface.

Console path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

2.23.20.26 Blink mode

In this table, you configure the blink mode for the physical WLAN interfaces.

Console path:

Setup > **Interfaces**

2.23.20.26.1 Ifc

Contains the name of the physical WLAN interface.

Console path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

WLAN-1
WLAN-2

2.23.20.26.2 Operating

Activates or deactivates the blink mode for this physical interface.

Console path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

Yes
No

Default:

No

2.23.20.26.3 Network

Here you select the logical WLAN interface that the device reports to the ERC.

Console path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

List of the available logical WLAN interfaces 'WLAN-1' to 'WLAN-x'

2.23.20.27 Starting an environment scan at a configurable time

This table is used to specify the daily time when the frequency band of the corresponding interface is scanned for rogue APs. It is also possible to use the *CRON syntax* for this. The search relies on active scanning with probe requests as well as passive scanning for beacons.

It is not always possible to use active scanning, for example where a 5 GHz channel is not DFS-free.

Console path:

Setup > **Interfaces** > **WLAN**

2.23.20.27.1 Ifc

This table contains the available WLAN interfaces.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

1

WLAN-1

2

WLAN-2

2.23.20.27.2 Yes

Enables/disables the environment scan.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0

Not active

1

Active

Default:

0

2.23.20.27.6 Hours

Set the hours value for the time of the environment scan here.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0 … 23

Default:

3

2.23.20.27.7 Minutes

Set the minutes value for the time of the environment scan here.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0 … 59

Default:

0

2.23.20.27.8 Frequency band

Here you set the radio band for which your WLAN module performs an environment scan.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

2.4 GHz
Scans the 2.4 GHz frequency band.

5 GHz
Scans the 5 GHz frequency band.

2.4/5 GHz
Scans the 2.4 GHz and 5 GHz frequency bands.

Default:

2.4 GHz

2.23.20.27.9 Subbands-5GHz

Here you configure the subbands of your 5 GHz frequency band.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

1+2+3
1+2
1+3
2+3
1
2
3

Default:

1+2+3

2.23.20.27.10 Channel-List-2.4 GHz

Here you can limit the 2.4 GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 2.4 GHz frequency band.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

empty
The environment scan is performed for all channels in the 2.4 GHz frequency band.

1
The environment scan is performed for channel 1 in the 2.4 GHz frequency band.

2
The environment scan is performed for channel 2 in the 2.4 GHz frequency band.

3
The environment scan is performed for channel 3 in the 2.4 GHz frequency band.

4
The environment scan is performed for channel 4 in the 2.4 GHz frequency band.

5
The environment scan is performed for channel 5 in the 2.4 GHz frequency band.

6
The environment scan is performed for channel 6 in the 2.4 GHz frequency band.

7
The environment scan is performed for channel 7 in the 2.4 GHz frequency band.

8
The environment scan is performed for channel 8 in the 2.4 GHz frequency band.

9
The environment scan is performed for channel 9 in the 2.4 GHz frequency band.

10
The environment scan is performed for channel 10 in the 2.4 GHz frequency band.

11

The environment scan is performed for channel 11 in the 2.4 GHz frequency band.

12

The environment scan is performed for channel 12 in the 2.4 GHz frequency band.

13

The environment scan is performed for channel 13 in the 2.4 GHz frequency band.

2.23.20.27.11 Channel-List-5 GHz

Here you can limit the 5 GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 5 GHz frequency band.

Console path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

empty

The environment scan is performed for all channels in the 5 GHz frequency band.

36

The environment scan is performed for channel 36 in the 5 GHz frequency band.

40

The environment scan is performed for channel 40 in the 5 GHz frequency band.

44

The environment scan is performed for channel 44 in the 5 GHz frequency band.

48

The environment scan is performed for channel 48 in the 5 GHz frequency band.

52

The environment scan is performed for channel 52 in the 5 GHz frequency band.

56

The environment scan is performed for channel 56 in the 5 GHz frequency band.

60

The environment scan is performed for channel 60 in the 5 GHz frequency band.

64

The environment scan is performed for channel 64 in the 5 GHz frequency band.

100

The environment scan is performed for channel 100 in the 5 GHz frequency band.

104

The environment scan is performed for channel 104 in the 5 GHz frequency band.

108

The environment scan is performed for channel 108 in the 5 GHz frequency band.

112

The environment scan is performed for channel 112 in the 5 GHz frequency band.

116

The environment scan is performed for channel 116 in the 5 GHz frequency band.

120

The environment scan is performed for channel 120 in the 5 GHz frequency band.

124

The environment scan is performed for channel 124 in the 5 GHz frequency band.

128

The environment scan is performed for channel 128 in the 5 GHz frequency band.

132

The environment scan is performed for channel 132 in the 5 GHz frequency band.

136

The environment scan is performed for channel 136 in the 5 GHz frequency band.

140

The environment scan is performed for channel 140 in the 5 GHz frequency band.

2.23.21 LAN interfaces

This menu contains the settings for the LAN interfaces.

Console path:

Setup > **Interfaces**

2.23.21.1 Ifc

Here you select the LAN interface, from those available on the device, to which the subsequent settings are to apply.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

2.23.21.2 Connector

Select the network connection you will use to connect to your local network. If you select **Auto**, the device will automatically detect the connection used.

The LAN interfaces of the device are equipped with different types of hardware depending on the model. The first LAN interface supports up to 1000 Mbps in full-duplex mode. The second LAN interface supports a maximum of 100 Mbps in full-duplex mode.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

Auto
Auto-10
Auto-100
FD10B-TX
100B-TX
FD100B-TX
FD1000B-TX
Power-Down

Default:

Auto

2.23.21.3 MDI-Mode

This switch activates/deactivates the automatic crossover of send and receive wire pairs (Auto-MDIX) making it unnecessary use node/hub switches or crossover cables. In individual cases (e.g. with certain fiber-optic media converters) it may be necessary to deactivate this automatic function and fix the setting to crossed (MDIX) or non-crossed (MDI).

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

Auto
MDI
MDIX

Default:

Auto

2.23.21.5 Clock role

An Ethernet port working in 1000BASE-Tx mode requires a continuous stream of data between both connected partners in order to stay synchronized. The nature of this requires the two ends to have a synchronized clock to transmit data. IEEE 802.3 introduced the concept of a master and a slave for this type of connection. The master provides the clocking for data transmission in both directions while the slave synchronizes to this clock. The roles as clocking master and slave are allocated at the automatic negotiation phase. This aspect can normally be ignored since automatic negotiation mostly works very well. In some cases it may be necessary to influence master-slave negotiation. This is the purpose of the setting for the clock.

The LAN interfaces of the device are equipped with different types of hardware depending on the model. Setting the clocking role has no effect on the second LAN interface.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

Slave-Preferred

This is the recommended default setting for devices that are not used as a switch. During the negotiation phase, the port will attempt to negotiate the slave role. It will accept the role of master if necessary.

Master-Preferred

During the negotiation phase, the port will attempt to negotiate the master role. It will accept the role of slave if necessary.

Slave

The port is set to the role slave only. A connection will be refused if both connection partners use the role of slave.

Master

The port is set to the role master only. A connection will be refused if both connection partners use the role of master.

Default:

Slave-Preferred

2.23.21.6 MTU

This entry contains the status values for MTU.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

2.23.21.7 Operating

Activate or deactivate the corresponding LAN interface here.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.23.21.8 Tx-Limit

Enter the bandwidth limit (kbps) in the transmission direction. The value 0 means there is no limit.

SNMP ID: 2.23.21.8

Telnet path: /Setup/Interfaces/LAN-Interfaces

Possible values:

› Maximum 10 numerical characters

Default: 0

This setting is only available for devices with a WLAN module.

2.23.21.9 Rx-Limit

Enter the bandwidth limit (kbps) in the receive direction.

This setting is only available for devices with a WLAN module.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

Bandwidth restriction revoked

2.23.21.10 Power-saving

Enter the bandwidth limit (kbps) in the receive direction.

This setting is only available for devices with a WLAN module.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.23.21.11 Flow control

Using flow control, you can prevent the loss of data packets if a partner network cannot process incoming data packets, for example due to a memory overflow. In this case, the receiver signals the sender to pause the data transmission for a certain period of time.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

Auto

If auto-negotiation is enabled, the flow control is performed automatically according to the capabilities of the partner (symmetric, asymmetric).

If auto-negotiation is disabled, no flow control takes place.

On

Enables symmetrical flow control when auto-negotiation is disabled.

Off

Disables the flow control when auto-negotiation is enabled.

2.23.23 PON

This menu contains the settings for the PON (Passive Optical Network) interfaces.

GPON (Gigabit Passive Optical Network) is an optical transmission standard for fiber optic connections (FTTH). LANCOM offers GPON SFP modules for this purpose, which are available in LANCOM routers with SFP interface. The list of compatible devices can be found in the respective GPON SFP data sheet.

With a GPON module, the LANCOM router can be operated directly on the fiber optic connection of the provider without a separate modem. Please contact your provider if operation without modem and with SFP module is supported. Usually GPON modems are authenticated by serial number and/or GPON password, so operation without provider support is not possible.

Console path:

Setup > **Interfaces**

2.23.23.1 Interface

The PON interfaces available on the device. Select here the SFP interface in which the PON module is plugged, e.g. SFP-1.

Console path:

Setup > **Interfaces** > **PON**

2.23.23.3 Password

Enter the PON password here if your provider performs password authentication. Other terms for PON password are “ONT installation identifier” or “PLOAM password”. The password consists of either 10 octets in ASCII representation or 20 characters in hexadecimal representation. The password is empty by default.

You can get the PON password for your connection from your Internet provider.

Console path:

Setup > **Interfaces** > **PON**

Possible values:

Either 10 ASCII or 20 hexadecimal characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.23.23.4 Managed

Configure here if the modem should be managed by the operating system. In this case the system writes the PON password (recommended).

Console path:

Setup > **Interfaces** > **PON**

Possible values:

No
Yes

2.23.30 Ethernet ports

The Ethernet interfaces on any publicly accessible device can potentially be used by unauthorized persons to gain physical access to a network. The Ethernet interfaces on the device can be disabled to prevent this.

Console path:

Setup > **Interfaces**

2.23.30.1 Port

The name of the selected port.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

2.23.30.2 Connector

Select the network connection you will use to connect to your local network. If you select Auto, the device will automatically detect the connection used.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

Auto
Auto-100
10B-T
FD10B-TX
100B-TX
FD100B-TX
FD1000B-TX

Default:

Auto

2.23.30.3 Private mode

Once private mode is activated, this switch port is unable to exchange data directly with the other switch ports.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

No
Yes

Default:

No

2.23.30.4 Allocation

Here you select how this interface is to be used.

The default value depends on the particular interface or the hardware model.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

LAN-1 to LAN-n
The interface is allocated to a logical LAN.
DSL-1 to DSL-n
The interface is allocated to a DSL interface.

Idle

The interface is not allocated to any particular task, but it remains physically active.

Monitor

The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Ethereal can be connected to this port, for example.

Power down

The interface is deactivated.

2.23.30.5 MDI-Mode

This item is used to set the connection type of the switch port. The connection type is either selected automatically or it can be fixed as a crossed (MDIX) or not crossed (MDI) connection.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

Auto
MDI
MDIX

Default:

Auto

2.23.30.6 Clock role

An Ethernet port working in 1000BASE-Tx mode requires a continuous stream of data between both connected partners in order to stay synchronized. The nature of this requires the two ends to have a synchronized clock to transmit data. IEEE 802.3 introduced the concept of a master and a slave for this type of connection. The master provides the clocking for data transmission in both directions while the slave synchronizes to this clock. The roles of clocking master and slave are shared out in the automatic negotiation phase. This aspect can normally be ignored since automatic negotiation mostly works very well. In some cases it may be necessary to influence master-slave negotiation.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

Slave-Preferred

This is the recommended default setting for non-switch devices. During the negotiation phase, the port will attempt to negotiate the slave role. It will accept the role of master if necessary.

Master-Preferred

During the negotiation phase, the port will attempt to negotiate the master role. It will accept the role of slave if necessary.

Slave

The port is forced to negotiate the slave role. A connection will **not** be established if both connection partners are forced to negotiate the slave role.

Master

The port is forced to negotiate the master role. A connection will **not** be established if both connection partners are forced to negotiate the master role.

Default:

Slave-Preferred

2.23.30.7 Downshift

With this setting you enable or disable automatic adjustment of the connection speed to the employed infrastructure for the specified Ethernet port. By enabling downshift, you allow the device to operate an Ethernet link with a lower transmission rate if the available speed is lower due to the cabling.

If, for example, two Gigabit-capable devices are connected with a cable which is not fully wired, both devices will initially attempt to establish a Gigabit link. Since Gigabit Ethernet in contrast to Fast Ethernet (10 or 100 Mbit) requires all four pairs of wires, the connection will fail. In this case, the downshift feature makes it possible to automatically fall back to the maximum possible transmission rate of the cable.

You can check whether downshift is available for an Ethernet link in the status menu under **Ethernet-Ports** > **Ports**.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

No
Yes

Default:

No

2.23.30.8 Power-saving

Using this setting you enable or disable the "Green Ethernet" enhancements according to IEEE 802.3az.

In order for your device to use the corresponding enhancements for Ethernet connections, the connected device must also support IEEE 802.3az. You can check in the status menu under **LAN** > **Interfaces** > **Power-saving** whether this is the case.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

No
Yes

Default:

No

2.23.30.9 Flow control

Using flow control, you can prevent the loss of data packets if a partner network cannot process incoming data packets, for example due to a memory overflow. In this case, the receiver signals the sender to pause the data transmission for a certain period of time.

Console path:

Setup > **Interfaces** > **LAN-Interfaces**

Possible values:

Auto

If auto-negotiation is enabled, the flow control is performed automatically according to the capabilities of the partner (symmetric, asymmetric).

If auto-negotiation is disabled, no flow control takes place.

On

Enables symmetrical flow control when auto-negotiation is disabled.

Off

Disables the flow control when auto-negotiation is enabled.

2.23.30.10 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Interfaces** > **Ethernet-ports**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.23.31 SFP Ports

Here you can find settings for the SFP port interfaces of the device.

Console path:

Setup > **Interfaces**

2.23.31.1 Port

The name of the selected port.

Console path:

Setup > **Interfaces** > **SFP-Ports**

2.23.31.2 Autoneg-Bypass

If an optical peer is detected with Auto-Negotiation enabled, but the negotiation cannot be completed, attempt a connection without Auto-Negotiation as an alternative.

Console path:

Setup > **Interfaces** > **SFP-Ports**

Possible values:

Yes
No

2.23.40 Modem

Commands and options used for an optional external modem connected to the serial interface.

Console path:

Setup > **Interfaces**

2.23.40.1 Ring count

Ring count.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

0 … 99

Default:

1

2.23.40.2 Echo-Off-Command

When the modem echo is enabled, the external modem sends back every character it receives. The modem echo must be disabled in order for the external modem to function properly with the device described here. The device uses this command to disable the modem echo.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

E0

2.23.40.3 Reset-Command

The device uses this command to perform a hardware reset on the externally connected modem.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

&F

2.23.40.4 Init-Command

The device uses this command to initialize the external modem.

The device sends this sequence to the external modem after this has had a hardware reset.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

L0X1M1S0=0

2.23.40.5 Dial-Command

The device issues this command when the external modem is to dial a number. The device takes the telephone number from the list of remote stations and appends it to the string specified here.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

DT

2.23.40.6 Request-ID

The device uses this command to query the modem ID. The result is output in the modem status.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

I6

2.23.40.7 Answer-Command

The device uses this command to accept a call arriving at the external modem.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

A

2.23.40.8 Disconnect-Command

The device uses this command to terminate calls made by the external modem (hang up).

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

H

2.23.40.9 Escape-Sequence

The device uses this command sequence to transmit individual commands to the modem in the data phase.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 9 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

+++

2.23.40.10 Escape-Promt-Delay-(ms)

After the escape sequence, the device waits for the time set here before issuing the command to hang up.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

0 … 9999 Milliseconds

Default:

1000

2.23.40.11 Init.-Dial

The device sends the initialization sequence for dialing to the external modem before outputting the dial command.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.23.40.12 Init.-Answer

The device sends the initialization sequence for answering to the external modem before outputting the accept-call command.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.23.40.13 Cycletime-AT-Poll-(s)

When disconnected, the device checks the presence and correct functioning of the external modem by sending the string "AT" to the modem. If the modem is connected properly and working, it responds with "OK". The cycle time for the "AT-Poll" defines the time interval between checks.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

0 … 9 Seconds

Default:

1

2.23.40.14 AT-Poll-Count

If the external modem does not respond to the number of AT polls from the device set here, then the device performs a hardware reset for the external modem.

Console path:

Setup > **Interfaces** > **Modem**

Possible values:

0 … 9

Default:

5

2.23.41 Mobile

The settings for mobile telephony are located here.

Console path:

Setup > **Interfaces**

2.23.41.1 Profiles

This table contains the settings for the GPRS/UMTS profiles.

Console path:

Setup > **Interfaces** > **Mobile**

2.23.41.1.1 Profile

Specify here a unique name for this UMTS/GPRS profile. This profile can then be selected in the UMTS/GPRS WAN settings.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.23.41.1.2 PIN

Enter the 4-digit PIN of the mobile phone SIM card used at the UMTS/GPRS interface. The device needs this information to operate the UMTS/GPRS interface.

The SIM card logs every failed attempt with an incorrect PIN. The number of failed attempts remains stored even when the device is temporarily disconnected from the mains. After 3 failed attempts, the SIM card is locked from further access attempts. If this occurs, you usually need the 8-digit PUK or SuperPIN to unlock it.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 6 characters from `[0-9]`

Default:

empty

2.23.41.1.3 APN

Here you enter the name of the access server for mobile data services known as the APN (AP Name). This information is specific to your mobile telephony service provider, and you will find this information in the documentation for your mobile telephony contract.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.23.41.1.4 Network

If you have opted for manual mobile network selection, then the UMTS/GPRS interface will login only to the mobile network specified here with its full name.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.23.41.1.5 Select

Search Results Web results Voraussetzungen :: Künstlersozialkasse https://www.kuenstlersozialkasse.de>Set the preferred **Network selection** mode:

If you have opted for automatic mobile network selection, then the cellular networking interface will login to any available and valid cellular network. If you select manual mobile network selection, then the cellular interface will only login to the network specified under 2/23/41/1/4.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Auto

The cellular modem automatically logs into the mobile network that it last used successfully. If the device fails to login, the mobile interface automatically logs in to the home network (HPLMN) stored on the SIM card.

If the cellular modem is also unable to login to the home network stored on the SIM card, a PLMN list of preferred roaming partners on the SIM card is processed in sequence with attempted logins. The mobile interface then connects to the first available cellular network, regardless of the signal quality.

If none of the above networks is available, one of the available PLMN networks with a "good" signal quality is selected at random: Failing this, the PLMN networks with a sufficient signal quality are processed, in the descending order of signal quality.

As soon as the login process succeeds, the network will be used. There is no change of network unless a loss of connection occurs. The provider can however trigger a change of the cell and the access mode, if it considers this to be appropriate.

Manual

The mobile modem connects to the mobile phone network specified under 2/23/41/1/4 only.

Manual mobile network selection is especially suitable when the device is in stationary operation and you wish to prevent it from connecting to another undesirable or more expensive mobile phone network.

If the manually set mobile network is not available, no connection will be established because the cellular modem only ever logs in to the manually specified network.

With the setting **Manual** and the field 2/23/41/1/4 empty, following a scan, the CLI command

```
do /Status/Modem-Mobile/Scan-Networks -s
```

enters the best network found into the field 2/23/41/1/4.

S-auto

Selects the provider automatically, although a preferred provider can be specified.

With this method, the cellular modem initially logs in to the mobile network that is entered into the field 2/23/41/1/4. If the device fails to login, the cellular modem logs on to the home network (HPLMN) stored on the SIM card.

If the HPLMN is not available, then a method analogous to automatic network selection is used, whereby the device attempts to connect to the "operator controlled PLMN selector" (roaming partner), a randomly chosen good network, or the best weak network (in that order).

Quality

Uses the provider with the best signal.

Using a scan manually initiated in LANmonitor or from the command line, the cellular modem searches for all available cellular networks and logs into the one with the best signal quality. If this login process fails, the mobile interface uses the **semi-automatic** network selection.

CLI commands

```
do /Status/Modem-Mobile/Scan-Networks -s -f
```

This command initially disconnects any existing cellular WAN connection, it then performs an extended scan and the best network is selected and stored to the configuration.

This command is available in combination with **semi-automatic** and **manual** network selection. The stored network is also valid after restarting the device (cold/warm boot) until "Scan-Networks -s / -e" is executed, for all modes except **automatic**. The results of the scan can be viewed under **Status** > **Modem-Mobile** > **Network-List**.

```
do /Status/Modem-Mobile/Scan-Networks -e -f
```

This command initially disconnects any existing cellular WAN connection and it then performs an extended scan. The parameter -e ensures that the best network found is used, but it is not entered into the configuration. However, the entry is made in the status tree.

```
do /Status/Modem-Mobile/Scan-Networks -s
```

This command performs a network scan only when the WWAN connection is inactive.

A manual scan can be performed on a regular basis and automatically by making an entry in the cron table on the LANCOM router. Enter the command

```
do /Status/Modem-Mobile/Scan-Networks -s -f
```

into the configuration dialog.

LANmonitor

In LANmonitor, you perform the scans mentioned above by right-clicking with the mouse on the Network list and selecting the desired operation from the context menu. The scanning method **Disconnect and use best network** is the most effective.

Default:

Auto

2.23.41.1.6 Mode

Select the mobile networking transmission mode here.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Auto

Automatic selection of transmission mode

3G

UMTS operation only

2G

GPRS operation only

3G-2G

Combined UMTS-GPRS operation

4G

LTE operation only

4G-3G

Combined LTE-UMTS operation

4G-2G

Combined LTE-GPRS operation

Default:

Auto

2.23.41.1.7 QoS-downstream-data-rate

The transfer rates used by the UMTS connection should be entered here to ensure that the Quality of Service (QoS) functions in the firewall work properly.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

The interface is unrestricted and QoS mechanisms do not take effect.

2.23.41.1.8 QoS-upstream-data-rate

The transfer rates used by the UMTS connection should be entered here to ensure that the Quality of Service (QoS) functions in the firewall work properly.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

The interface is unrestricted and QoS mechanisms do not take effect.

2.23.41.1.9 PDP type

With this setting you specify the type of PDP context for the mobile profile. The PDP context describes the support of the address spaces which the backbone of the corresponding cellular network provider offers for connections from the cellular network to the Internet. This can be either IPv4 or IPv6 alone, or can include support for both address spaces (dual stack). Clients that want to use the corresponding cellular network provider must support at least one of the specified address spaces.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

IPv4
IPv6
IPv4v6

Default:

IPv4

2.23.41.1.10 Bands

If unfavorable environmental conditions cause the device to constantly switch between two frequency bands, instabilities in the transmission may be the result. This selection allows you to control which frequency bands the mobile networking device can or should use. The LTE bands that are available depend on the supported LTE bands, as listed in the data sheet of the respective product. The following frequency bands are available:

- **B1_2100**: Band 1 (2100MHz) is enabled.
- **B2_1900**: Band 2 (1900MHz) is enabled.
- **B3_1800**: Band 3 (1800MHz) is enabled.
- **B4_2100**: Band 4 (2100MHz) is enabled.
- **B5_850**: Band 5 (850MHz) is enabled.

- **B7_2600**: Band 7 (2600MHz) is enabled.
- **B8_900**: Band 8 (900MHz) is enabled.
- **B12_700**: Band 12 (700MHz) is enabled.
- **B13_700**: Band 13 (700MHz) is enabled.
- **B14_700**: Band 14 (700MHz) is enabled.
- **B17_700**: Band 17 (700MHz) is enabled.
- **B18_850**: Band 18 (850MHz) is enabled.
- **B19_850**: Band 19 (850MHz) is enabled.
- **B20_800**: Band 20 (800MHz) is enabled.
- **B25_1900**: Band 25 (1900MHz) is enabled.
- **B26_800**: Band 26 (800MHz) is enabled.
- **B28_700**: Band 28 (700MHz) is enabled.
- **B29_700**: Band 29 (700MHz) is enabled.
- **B30_2300**: Band 30 (2300MHz) is enabled.
- **B32_1500**: Band 32 (1500MHz) is enabled.
- **B34_2000**: Band 34 (2000MHz) is enabled.
- **B38_2600**: Band 38 (2600MHz) is enabled.
- **B39_1900**: Band 39 (1900MHz) is enabled.
- **B40_2300**: Band 40 (2300MHz) is enabled.
- **B41_2600**: Band 41 (2600MHz) is enabled.
- **B42_3500**: Band 42 (3500MHz) is enabled.
- **B43_3700**: Band 43 (3700MHz) is enabled.
- **B46_5200**: Band 46 (5200MHz) is enabled.
- **B48_3500**: Band 48 (3500MHz) is enabled.
- **All**: All frequency bands are enabled.

This option applies only to the 4G/5G-standard frequency bands. All bands can be used for UMTS and GPRS.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

All
B1_2100
B2_1900
B3_1800
B4_2100
B5_850
B7_2600
B8_900
B12_700
B13_700
B14_700
B17_700
B18_850
B19_850
B20_800
B25_1900
B26_800
B28_700
B29_700
B30_2300
B32_1500
B34_2000
B38_2600
B39_1900
B40_2300
B41_2600
B42_3500
B43_3700
B46_5200
B48_3500

2.23.41.1.13 Bands2

Further LTE bands as a supplement to *2.23.41.1.10 Bands* on page 873.

- **B66_1700**: Band 66 (1700MHz) is enabled.
- **B70_1600**: Band 70 (1600MHz) is enabled.
- **B71_600**: Band 71 (600MHz) is enabled.
- **B75_1400**: Band 75 (1400MHz) is enabled.
- **B76_1400**: Band 76 (1400MHz) is enabled.
- **B77_3700**: Band 77 (3700MHz) is enabled.
- **B78_3500**: Band 78 (3500MHz) is enabled.
- **B79_4700**: Band 79 (4700MHz) is enabled.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

B66_1700
B70_1600
B71_600
B75_1400
B76_1400
B77_3700
B78_3500
B79_4700

2.23.41.1.14 APN-Mode

Defines in which mode the APN is to be used.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Auto

With Automatic, the APN is taken from the internal database of the provider settings of the operating system. For this purpose, the provider is queried from the SIM card (MCC/MNC) and searched for in the internal database. The "Automatic" mode only works with public provider APNs and not with private APNs. For private APNs, the mode must be set to "Manual" and the APN entered in the field *2.23.41.1.3 APN* on page 869.

Manual

For Manual, the APN from the field *2.23.41.1.3 APN* on page 869 is used.

Default:

Auto

2.23.41.1.15 Cold-Standby

Specifies whether the cellular modem should be logged into the cellular network in non-backup cases. If "Yes" the cellular modem is not logged into the cellular network in the non-backup case. In the case of a backup, it takes correspondingly longer for the module to fully establish a backup connection. This function is only supported if the backup table is used. This function has no effect or cannot be used when working with administrative distances, since in that case the WWAN modem has always established an active data connection.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Yes
No

Default:

No

2.23.41.1.16 Roaming-PDP-Type

Defines with which PDP type (IPv4, IPv6 or IPv4 and IPv6) the mobile connection is to be established in the case of roaming.

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

IPv4
IPv6
IPv4v6

Default:

IPv4

2.23.41.1.17 Data-Roaming

Activates or deactivates the data connection if the device is logged into a foreign mobile network (roaming).

Console path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Yes
No

Default:

Yes

2.23.41.2 Scan networks

This command starts a scan for available networks. The networks discovered are listed as a network list under the modem status.

Console path:

Setup > **Interfaces** > **Mobile**

2.23.41.3 Input PUK

If PIN entry is locked after multiple entries of the wrong number (e.g. because the profile is incorrect), the SIM card must be activated again by entering the PUK. This command starts the the PUK entry procedure.

Console path:

Setup > **Interfaces** > **Mobile**

2.23.41.6 History interval (sec)

Logging interval in seconds for the values displayed for the modem status under History.

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

0 … 999999 Seconds

Default:

0

Special values:

0

The value "0" disables the logging of history values.

2.23.41.7 SYSLOG enabled

Activate this option if the history values for modem status (also see "2 .23.41.6 History interval (sec)") are additionally to be logged by SYSLOG.

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

No
Yes

Default:

No

2.23.41.8 Enable HSUPA

HSUPA can be activated or deactivated here.

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

No
Yes

Default:

Yes

2.23.41.9 Signal check interval (min)

This value specifies the time in minutes after which the device may switch back a 3G connection (if available).

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

0 … 9999 Minutes

Default:

0

Special values:

0

The value "0" disables the fallback from 3G to 2G connections.

2.23.41.10 Threshold 3G-to-2G (dB)

This value specifies the threshold for falling back from 3G to 2G connections. If the signal strength in 3G mode falls below this threshold, then the device switches to a 2G connection (if available). Positive values are automatically converted into negative values.

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

-51 … -111 dB

Default:

-89

Special values:

0

The value "0" disables the fallback from 3G to 2G connections.

2.23.41.11 Check-while-connected

Activate this option if the device is also to be allowed to fallback to 2G connections when WAN connections exist.

This setting only takes effect if the fallback from 3G to 2G connections has been configured.

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

No
Yes

Default:

Yes

2.23.41.12 PIN-change

This action changes the PIN of the SIM card in your device. Syntax:

```
do pin-change <old_PIN><new_PIN> <new_PIN>
```

Console path:

Setup > **Interfaces** > **Mobile**

Possible values:

4 characters from `[0-9]`

2.23.41.13 Signal thresholds

This menu contains the signal thresholds.

Console path:

Setup > **Interfaces** > **Mobile**

2.23.41.13.1 Index

Here you set the index.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.2 Status

Here you set the status.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.3 RSRP

Here you set the RSRP.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.4 RSCP

Here you set the RSCP.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.5 RSSI

Here you set the RSSI.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.6 MCC

Specify the Mobile Country Code (MCC) here. Each country has its own country code. For Germany this is 262.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.13.7 MNC

Specify the Mobile Network Code (MNC) here. This identifies the mobile network provider. For example, 01 in Germany refers to Deutsche Telekom.

Console path:

Setup > **Interfaces** > **Mobile** > **Signal-Thresholds**

2.23.41.14 Syslog

This menu contains entries that may trigger syslog messages.

Console path:

Setup > **Interfaces** > **Mobile**

2.23.41.14.1 Syslog-Signal-Hysteresis

Defines at how much dB difference in signal level fluctuations (previous value to current value) a syslog message should be generated.

Console path:

Setup > **Interfaces** > **Mobile** > **Syslog**

Possible values:

Max. 4 characters from `[0-9]`

Default:

5

2.23.51 Analog

This table contains the configuration of the analog interfaces.

Console path:

Setup > **Interfaces**

2.23.51.1 Ifc

This entry contains the name of the analog interface (e.g. Analog-1).

Console path:

Setup > **Interfaces** > **Analog**

2.23.51.2 Operating

This entry enables or disables the analog interface.

Console path:

Setup > **Interfaces** > **Analog**

Possible values:

No

The analog interface is deactivated.

Yes

The analog interface is activated.

Default:

Yes

2.23.51.3 Microphone gain

This entry controls the microphone gain.

Console path:

Setup > **Interfaces** > **Analog**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

-2

2.23.51.4 Speaker gain

This entry controls the speaker gain.

Console path:

Setup > **Interfaces** > **Analog**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

-11

2.23.51.5 Line-Disruption

Occasionally analog modems do not hang up even though the caller has ended the connection. In this state, the modem is unable to accept a new connection. If the analog port is off-hook but in the idle state, the corresponding port is briefly deactivated and reactivated after the time set here in seconds. This interrupts the voltage on the end device, causing the telephone/modem to terminate the connection.

Console path:

Setup > **Interfaces** > **Analog**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

Deactivates the autom. switch-off.

2.23.52 Monitor-Capacity

This menu contains the configuration options for the monitoring of the interfaces.

Console path:

Setup > **Interfaces**

2.23.52.1 Warning

This entry enables or disables the settings for the interface-monitoring warnings.

Console path:

Setup > **Interfaces** > **Monitor-Capacity**

Possible values:

No
Yes

Default:

Yes

2.23.52.2 E-mail

Here you specify the e-mail address of the recipient of alert messages.

Console path:

Setup > **Interfaces** > **Monitor-Capacity**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.23.90 Bluetooth

This menu allows you to configure Bluetooth devices.

Console path:

Setup > **Interfaces**

2.23.90.1 iBeacon

This entry allows you to configure the iBeacon module.

Console path:

Setup > **Interfaces** > **Bluetooth**

2.23.90.1.1 Operating

This entry allows you to set the operating mode of the module.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Off

The module is not enabled.

Manual

iBeacon configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Managed

2.23.90.1.2 UUID

This entry allows you to assign a "universally unique identifier" (UUID) to the iBeacon module.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 36 characters from `[0-9][a-f][A-F]-`

Default:

00000000-0000-0000-0000-000000000000

2.23.90.1.3 Major

Assign a unique major ID to the iBeacon module.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

2002

2.23.90.1.4 Minor

Assign a unique minor ID to the iBeacon module.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

1001

2.23.90.1.5 Reception power shift

Specify the reception power shift.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 4 characters from `[0-9]-`

-128 … 127

Default:

0

2.23.90.1.6 Transmission power

Set the transmission power of the iBeacon module.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Low
The module sends with minimum power.

Medium
The module sends with medium power.

High
The module sends with maximum power.

Default:

High

2.23.90.1.7 Channel/channels

Set which channels the iBeacon module should use to transmit.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

2402MHz
The module transmits on channel 2402.

2426MHz
The module transmits on channel 2426.

2480MHz
The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz
The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

2.23.90.1.8 Coexistence

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

No
Yes

Default:

Yes

2.23.90.1.9 Module restart

This command causes the iBeacon module to restart.

Console path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

2.24 Public-Spot-Module

This menu contains the settings for the Public Spot.

Console path:

Setup

2.24.1 Authentication-Mode

Your device supports different types of authentication for network access with a Public Spot. To start with, you can specify whether a user needs to log in at all. The Public Spot stores the credentials in the user table. If you choose to use a registration procedure, you have two options:

- Login is performed with either a username and password, or additionally with the physical or MAC address. In this case, the administrator communicates the access credentials to the users by means of a printout.
- The login is performed using the username and password, which the user generates themself. Access credentials can be automatically sent to users that login for first time either by e-mail or SMS (text message).
- The login is automatically performed via a RADIUS server after the user has accepted the terms of use on the welcome page that the administrator set up. The access credentials remain hidden from the user, and the user does not need them. The creation of a user account on the RADIUS server is only for the internal administration of the associated users.

Console path:

Setup > **Public-Spot-Module**

Possible values:

None
User+password
MAC+user+password
E-mail
E-Mail2SMS
Login-via-agreement

Default:

None

2.24.3 RADIUS-Servers

When you configure a public spot, the user credentials for authentication and for accounting can be forwarded to one or more RADIUS servers. These are configured in the provider list.

In addition to the dedicated parameters for the RADIUS providers, you must enter the general RADIUS parameters, such as the retry and timeout values, into the appropriate configuration areas.

Console path:

Setup > **Public-Spot-Module**

2.24.3.1 Provider

Name of the RADIUS server provider who supplies the authentication and/or accounting.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.3.3 Auth.-Server-Port

Enter here the valid port used by the server that the Public Spot requests for authenticating the access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 5 characters from `[0-9]`

Default:

10

2.24.3.4 Auth.-Server-Secret

Enter here the key (shared secret) for access to the RADIUS server of the provider. Ensure that this key is consistent with that in the RADIUS server.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.24.3.6 Acc.-Server-Port

Enter here the valid port used by the server that the Public Spot uses for the accounting of the access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 5 characters from `[0-9]`

Default:

10

2.24.3.7 Acc.-Server-Secret

Enter here the key (shared secret) for access to the accounting server of the provider. Ensure that this key is consistent with that in the accounting server.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.24.3.8 Backup

From the list of specified RADIUS providers, select a different entry from the provider table for use as a backup. If the server at the primary provider is unavailable, the Public Spot contacts the backup provider for authentication and/or accounting of access sessions.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.3.9 Auth.-Server-Loopback-Addr.

Enter here the loopback address of the server that the Public Spot contacts for authenticating the access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Name of the IP networks whose addresses are to be used.

INT

The address of the first intranet.

DMZ

The address of the first DMZ.

LBO…LBF

The 16 loopback addresses.

Any valid IP address

2.24.3.10 Acc.-Server-Loopback-Addr.

Enter here the loopback address of the server that the Public Spot contacts for accounting the access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Name of the IP networks whose addresses are to be used.

INT

The address of the first intranet.

DMZ

The address of the first DMZ.

LBO…LBF

The 16 loopback addresses.

Any valid IP address

2.24.3.11 Auth.-Server-Protocol

This item selects the protocol that the Public Spot is to use for authenticating access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.24.3.12 Acc.-Server-Protocol

This item selects the protocol that the Public Spot is to use for the accounting of the access sessions with this provider.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

2.24.3.13 Auth.-Server-Hostname

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server which the Public Spot contacts for authentication with this provider.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

2.24.3.14 Acc.-Server-Hostname

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server which the Public Spot contacts for accounting the access sessions with this provider.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

2.24.3.15 Auth.-Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers** > **Server**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.3.16 Acc.-Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **Public-Spot-Module** > **RADIUS-Servers** > **Server**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.5 Traffic-Limit-Bytes

Even before login and quite independent of the servers, networks and pages mentioned earlier, traffic is generated by DHCP, DNS and ARP requests. These requests are allowed. However, they can be misused to tunnel other data.

To counter this, you can define a maximum transfer volume here. This affects only the data exchanged before login and not the data sent to or from the free web servers mentioned above. This remains unlimited at all times.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.24.6 Server-Subdir

Enter the directory for the public page used by your Public Spot service. This page should provide information enabling the new user to contact you and register.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.7 Accounting-Cycle

Define the time in seconds for the accounting cycle.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.24.8 Page-Table

In addition to freely available web servers, you can define customized pages which your customers can access without having to log on.

The page table allows you to link certain pre-defined events with certain pages on your servers, so that when these events occur the standard pages are displayed.

Console path:

Setup > **Public-Spot-Module**

2.24.8.1 Page

Name of the page that your customers can use without logging in.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

2.24.8.2 URL

URL of the page that your customers can use without logging in.

By default, different HTML pages stored on the device file system can be displayed, depending on the page chosen by the user.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.8.3 Fallback

Enable or disable the fallback to the "on-board" page in case the Public Spot cannot display the user-defined URL.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

Possible values:

No
Yes

Default:

No

2.24.8.4 Type

Select the type of the page.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

Possible values:

Template
Redirect

Default:

Template

2.24.8.5 Loopback-Addr.

Enter a loopback address.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

Possible values:

Name of the IP networks whose addresses are to be used.
INT

The address of the first intranet.

DMZ

The address of the first DMZ.

LBO…LBF

The 16 loopback addresses.

Any valid IP address

2.24.8.6 Template-Cache

Using this parameter, you enable caching of Public Spot templates.

When configuring user-defined template pages on devices with sufficient memory (e.g., Public Spot gateways), you have the option to cache templates on the device. Caching improves the performance of the Public Spot module, particularly in large-scale scenarios where the device internally caches templates and the HTML pages that were generated from them.

Caching is possible for:

- Templates stored in the local file system
- Templates stored on external HTTP(S) servers with static URLs

Templates on external servers that are referenced with template variables are not cached on the system.

Console path:

Setup > **Public-Spot-Module** > **Page-Table**

Possible values:

No
Yes

Default:

No

2.24.9 Roaming-Secret

When moving into the signal coverage area of another base station (roaming), it is necessary to login again. If you are located in the overlap area between two stations, you may even experience a regular change of connection between the two base stations. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.12 Communication-Port

Here you set the valid port that the Public Spot uses to communicate with the clients associated with it.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.24.14 Idle-Timeout

If an idle timeout has been defined (either here or by RADIUS) the Public Spot terminates the connection if no data was received from the client within the specified interval.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.24.15 Port-Table

This table is used to activate or deactivate the authentication by Public Spot for the ports on the device.

Console path:

Setup > **Public-Spot-Module**

2.24.15.2 Port

Select the port (e.g. LAN-1) for which you want to activate or deactivate authentication by the Public Spot.

Console path:

Setup > **Public-Spot-Module** > **Port-Table**

2.24.15.3 Authentication-Necessary

Activate or deactivate authentication by the Public Spot for the selected port.

Console path:

Setup > **Public-Spot-Module** > **Port-Table**

Possible values:

No
Yes

Default:

No

2.24.15.4 Description

Field for a description of the port. This field is also used for the cloud-managed hotspot feature of the LANCOM Management Cloud to uniquely identify the hotspot. In this case, the LANCOM Management Cloud stores a UUID here.

Console path:

Setup > **Public-Spot-Module** > **Port-Table**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.24.16 Auto-Cleanup-User-Table

This item specifies whether the user list is automatically cleaned up. Since the size of the user table is limited, outdated user accounts should be deleted as soon as possible.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

No

2.24.17 Provide-Server-Database

Here you can select whether the Public Spot provides the MAC address list via RADIUS.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

No

2.24.18 Disallow-Multiple-Login

Allows a single user account to login multiple times simultaneously.

The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

No

2.24.19 Add-User-Wizard

This wizard in WEBconfig provides you with an easy way to create Public Spot user accounts. The wizard automatically generates a username and password and then presents a page for printing out with all the necessary credentials. This menu contains the settings for this wizard.

Console path:

Setup > **Public-Spot-Module**

2.24.19.2 Username-Pattern

This item defines the format of the name of new user accounts.

The string "%n" is a placeholder for a unique account number that is automatically generated by the Public Spot.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Max. 19 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

user%n

2.24.19.3 Password-Length

Define the length of the password generated for a new account by the Public Spot Add-User wizard.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

0 … 255

Default:

6

2.24.19.5 Default-Runtime

In this table, you define the optional default runtimes as presented by the Public Spot Add-User wizard. The wizard offers these options when you create a user account.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

2.24.19.5.1 Runtime

Select the runtime of a user account on the Public Spot.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Default-Runtime**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.24.19.5.2 Unit

Select the unit to be used for the runtime of a user account on the Public Spot.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Default-Runtime**

Possible values:

Minute(s)
Hour(s)
Day(s)

Default:

Hour(s)

2.24.19.6 Comment-Fields

In this table, you define the comment fields for the Public Spot Add-User wizard.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

2.24.19.6.1 Field-Name

The Public Spot Add-User wizard can print out up to 5 comments on the form. This item is used to set the names of the comment fields that are displayed by the wizard when creating the user accounts.

Activate the printout of the comments with the option *2.24.19.8 Print-Comments-on-Voucher* on page 903.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Comment-Fields**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.19.7 Default-Starting-Time

Specify the default starting time here.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Immediately
First login

Default:

First login

2.24.19.8 Print-Comments-on-Voucher

This item activates or deactivates the printout of the comment fields on the voucher for a Public Spot user.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

No

2.24.19.9 Maximal-Voucher-Validity-Period

This value defines the maximum validity period of the voucher in days.

If you starting time for the voucher's runtime to "first login" (*2.24.19.7 Default-Starting-Time* on page 902), the runtime for the vouchers will begin at some time in the future. The maximum validity period takes precedence over the runtime of the individual voucher. If the user activates the voucher, the runtime could potentially have expired already or could expire during the intended runtime.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Max. 31 characters from `[0-9]`

Default:

365

2.24.19.10 Available-expiry-methods

Use this setting to determine which expiry methods are offered by the Public-Spot add-user wizard when creating new user accounts.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

All methods

The wizard offers all of the available expiry methods.

Current time method

The expiry method offered by the wizard is based on the current time. The runtime of a user account created with this method begins immediately when the user account is created.

Login-time-method

The expiry method offered by the wizard is based on the login time. The runtime of a user account created with this method begins when the user logs in to the Public Spot for the first time.

If you select this method, the user account could feasibly expire before the user has logged in for the first time if this time is longer than the maximum voucher validity period (*2.24.19.9 Maximal-Voucher-Validity-Period* on page 903).

Default:

All methods

2.24.19.11 SSID-Table

This table contains the list of network names available for Public Spot users.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

2.24.19.11.1 Network-Name

This table contains the list of network names available for Public Spot users.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **SSID-Table**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.19.11.2 Default

Specifies the name of the wireless LAN as the default value. The Create Public Spot Account Wizard will automatically suggest this value in the list of available WLAN networks. You can optionally change this value in the Wizard's input mask.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **SSID-Table**

Possible values:

No
Yes

Default:

No

2.24.19.12 User-name-case-sensitive

This setting specifies whether the name of the newly created Public Spot user is handled case-sensitive.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

Yes

2.24.19.13 Hide-Case-Sensitive-Checkbox

This setting determines whether the option for the case-sensitive input of user names is visible in the Public-Spot add-user wizard.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

Yes

2.24.19.14 Max-Concurrent-Logins-Table

With this table you can set the number of devices that can simultaneously access each account; this is done by entering one or several values. By entering different values (e.g. 1, 3, 4, 5) you can respond to the needs of different users or user groups.

The valeu "0" enables an unlimited number of logins for a single account.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0, 3, 10

2.24.19.14.1 Value

Using this entry you define a default value for the selection menu **Max-Concurrent-Logins**, which you can find in the setup wizard **Create Public Spot account**. The specified value describes the maximum number of devices which can be logged in at the same time using a single user account. The value `0` stands for "unlimited".

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Max-Concurrent-Logins-Table**

Possible values:

0 … 99999

Default:

empty

2.24.19.15 Multi-Login

Using this setting you specify whether multiple login, which you create with the setup wizard **Create Public Spot account** or via web API (without entering variables/values) is allowed by default. In the setup wizard, for example, the option field **Multiple-Logins** is preselected by default.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

No

2.24.19.16 Hide-Multi-Login-Checkbox

Using this setting you hide the option field **Multi-Login** in the setup wizard **Create Public Spot account**.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

No

2.24.19.17 Bandwidth-Profiles

In this table you manage individual bandwidth profiles. Using a bandwidth profile you have the option to selectively restrict the bandwidth (uplink and downlink) that is available to Public Spot users when their accounts are created.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

2.24.19.17.1 Profile-Name

Enter the name for the bandwidth profile here.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.19.17.2 TX-Bandwidth

Enter the maximum uplink bandwidth (in bps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

Possible values:

0 … 4294967295 Bps

Default:

0

2.24.19.17.3 RX-Bandwidth

Enter the maximum uplink bandwidth (in bps), which should be available to Public Spot users. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

Possible values:

0 … 4294967295 Bps

Default:

0

2.24.19.18 Password-Character-Set

This setting specifies the character set used by the **Create Public Spot Account** wizard to create passwords for new users.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Character+digits
Characters
Digits

2.24.19.19 Hide-CSV-Export

This parameter determines whether or not to display the button for exporting information to a CSV file in the Wizard for creating new Public Spot accounts.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

No

2.24.19.20 Hide-User-Management-Button

This parameter gives you the option to hide the **Manage user wizard** button in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Yes

The **Create Public Spot account** Setup Wizard hides the **Manage user wizard** button.

No

The Setup Wizard displays the **Manage user button**.

Default:

No

2.24.19.21 Maximal-Voucher-Validity-Period-Unit

Use this entry to specify the units to be used for the maximum voucher validity period.

Console path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Minute(s)

Specifies that the validity period is entered as minutes.

Hour(s)

Specifies that the validity period is entered as hours.

Day(s)

Specifies that the validity period is entered as days.

Default:

Day(s)

2.24.20 VLAN-Table

By default, all data is routed via the relevant interface. However if VLAN-ID tags are specified, the only data to be routed via the relevant interface is that tagged with the specified VLAN-ID. Only select VLAN-IDs here if you do not want all data packets to be routed via the corresponding interface.

Console path:

Setup > **Public-Spot-Module**

2.24.20.1 VLAN-ID

By default, all data is routed via the relevant interface. However if VLAN-ID tags are specified, the only data to be routed via the relevant interface is that tagged with the specified VLAN-ID. Only select VLAN-IDs here if you do not want all data packets to be routed via the corresponding interface.

Console path:

Setup > **Public-Spot-Module** > **VLAN-Table**

Possible values:

0 … 4096

Default:

empty

2.24.21 Login-Page-Type

Here you select the protocol to be used by the Public Spot to display the login pages.

Console path:

Setup > **Public-Spot-Module**

Possible values:

HTTP
HTTPS

Default:

HTTP

2.24.22 Device-Hostname

Certificates are normally issues for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address. This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.23 MAC-Address-Table

This table contains the WLAN clients that can automatically authenticate to the Public Spot using the MAC address.

Console path:

Setup > **Public-Spot-Module**

2.24.23.1 MAC-Address

The valid MAC address of the WLAN client that is able to use automatic authentication.

Console path:

Setup > **Public-Spot-Module** > **MAC-Address-Table**

Possible values:

Max. 12 characters from `[A-F][a-f][0-9]`

Default:

000000000000

2.24.23.2 User-Name

User name of the WLAN client that can use automatic authentication. The Public Spot takes this name for the optional session accounting by means of RADIUS server.

Console path:

Setup > **Public-Spot-Module** > **MAC-Address-Table**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.23.3 Provider

The Public Spot uses this provider for the optional session accounting by means of RADIUS server. To this end, enter a RADIUS server that is specified in the provider list.

Console path:

Setup > **Public-Spot-Module** > **MAC-Address-Table**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.24 MAC-Address-Check-Provider

The Public Spot uses this provider to authenticate the MAC address by means of RADIUS server. To this end, enter a RADIUS server that is specified in the provider list.

If no provider is selected, no authentication of the MAC address by RADIUS server takes place. In this case, only those WLAN clients listed in the MAC address table can authenticate at the Public Spot without logging on.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.25 MAC-Address-Check-Cache-Time

If a MAC address authentication is rejected by the RADIUS server, the Public Spot saves this rejection for the lifetime defined here (in seconds). The Public Spot responds directly to further requests for the same MAC address, without forwarding it to the RADIUS server first.

Console path:

Setup > **Public-Spot-Module**

Possible values:

0 … 4294967295 Seconds

Default:

60

2.24.26 Station-Table-Limit

You can increase the maximum number of clients up to 65,536.

While the device is operating, changes to the station table only come into immediate effect if the table has been extended. Restart the access point in order to immediately reduce the size of the station table.

Console path:

Setup > **Public-Spot-Module**

Possible values:

16 … 65536 Seconds

Default:

8192

2.24.30 Free-Server

Enter the IP address of the public page used by your Public Spot service. This page should provide information enabling the new user to contact you and register.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.31 Free-Networks

In addition to freely available web servers, you can define other networks which your customers can access without having to log on. As of LCOS version 8.80 you also have the option to enter the hostname using wildcards.

Console path:

Setup > **Public-Spot-Module**

2.24.31.1 Host-Name

With this input field in the **Free networks** table, you can define a server, network, or individual web pages, which customers may use without a login. Here you can enter either an IP-address or a host name, both of which allow the use of wildcards. This allows you to enter values such as "203.000.113.*", "google.??*" or "*.wikipedia.org". The table is dynamic and the display is adjusted according to the number of host names and IP addresses that you enter.

Console path:

Setup > **Public-Spot-Module** > **Free-Networks**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]*-?.`

Default:

empty

2.24.31.2 Mask

Enter the associated netmask here. If you wish to authorize just a single workstation with the previously specified IP address, enter `255.255.255.255` here. If you wish to authorize a whole IP network, enter the corresponding netmask.

Console path:

Setup > **Public-Spot-Module** > **Free-Networks**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.24.31.3 VLANs

This parameter optionally defines a list of VLAN IDs which control the approved site(s) that are available to the corresponding host name. Only users who have the VLAN ID stored in the station table are able to access this host without having to authenticate. Use this parameter, for example, in application scenarios where Public Spot networks/SSIDs are separated by VLAN and you wish to set different access restrictions for different user groups.

Console path:

Setup > **Public-Spot-Module** > **Free-Networks** > **VLans**

Possible values:

Default:

empty

Comma-separated list, max. 16 characters from `[0-9],`

Special values:

empty, **0**

Access to the host entered here is possible from all VLANs.

2.24.32 Free-Hosts-Minimum-TTL

The configuration of the Public Spots can allow users to visit unlocked web pages, web servers or networks, free of charge and without requiring a login. The access point directs the visitors to the IP addresses corresponding to the host name. The access point saves the host names and the corresponding IP addresses in the state tables **Status** > **Public-Spot** > **Free-hosts** and **Status** > **Public-Spot** > **Free-networks**.

This value specifies the time in seconds for which the addresses in the status table **Free hosts** are valid (TTL: "Time to live").

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 10 characters from `[0-9]`

Default:

300

Special values:

0

The validity period is set by the duration in the DNS response (TTL).

2.24.34 WAN-Connection

With this parameter you name the remote station that is monitored by the Public Spot module for its connection status, in order to display an appropriate message to unauthenticated users in the case of a WAN-link failure. Potential users are informed about the lack of network availability beforehand.

If no remote site is named for monitoring, the Public Spot module disables the display of the connection error page. If the WAN connection fails, unauthenticated will not see an error page and their browsers will timeout instead.

Users who are already authenticated will see an appropriate error message from their browser.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.35 Print-Logo-And-Headerboard

In the default settings, the device outputs a voucher with the header image "Hotspot" and the logo "Powered by LANCOM". You have the option of disabling these graphics directly on the device without having to upload a customized version of the voucher template without the graphics. If you disable the graphics, a text-only voucher is issued.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

Yes

2.24.36 User-Must-Accept-GTC

Enabling this parameter allows you to combine certain login modes with an acceptance of the terms and conditions. In this case, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering or logging in. Users who do not explicitly agree to these terms and conditions are unable to login to the Public Spot.

The following login modes can be combined with an acceptance of the terms and conditions:

- User+password
- MAC+user+password
- E-mail
- E-Mail2SMS

Remember to upload a page with the terms and conditions onto the device before you require them to be confirmed.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

No

2.24.37 Print-Logout-Link

This parameter determines whether a voucher printout shows the URL for logging out from the Public Spot.

Iin order for the correct URL to appear on the voucher, the parameter **Device host name** (SNMP ID 2.24.22) must contain the value `logout`.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

Yes

2.24.38 LBS-Tracking

Here you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
Yes

Default:

No

2.24.39 LBS-Tracking-List

Name of the LBS tracking list.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.40 XML-Interface

Configure the XML interface here.

Console path:

Setup > **Public-Spot-Module**

2.24.40.1 Operating

Enable the XML interface here.

Console path:

Setup > **Public-Spot-Module** > **XML-Interface**

Possible values:

No
Yes

Default:

No

2.24.40.2 Radius-Authentication

This item enables or disables authentication by a RADIUS server when using the XML interface of the Public Spot.

The additional authentication by RADIUS server is only active if the Public Spot's XML interface is enabled.

Console path:

Setup > **Public-Spot-Module** > **XML-Interface**

Possible values:

No

No additional authentication necessary.

Yes

The Public Spot forwards the request to the internal RADIUS server, or a RADIUS re-direct transfers it via a realm to an external RADIUS server.

Default:

Yes

2.24.41 Authentication-modules

In this menu option you define individual parameters for using the network login, and you specify how and with what parameters the authentication is performed and the login data is transmitted.

Console path:

Setup > **Public-Spot-Module**

2.24.41.1 E-mail-Authentication

This menu specifies the settings for authentication to the network and transmission of the credentials. The latter is done by e-mail.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

2.24.41.1.1 Limit-e-mails-per-Hour

Enter the maximum number of e-mails sent within one hour to Public-Spot users with login data.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Max. 5 characters from `[0-9]`

Default:

100

2.24.41.1.5 Max-Request-Attempts

With this parameter you specify how many different credentials can be requested for a MAC address within one day.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3

2.24.41.1.6 Local-e-mail-Address

Enter the valid sender e-mail address for the e-mail that is sent.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.8 Black-White-Domain-List

With this parameter you specify whether the device uses the table **Domain-List** as a blacklist or whitelist. This definition sets which e-mail addresses or domains may be entered by your Public Spot users in order to register.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Blacklist

Registration is permitted on all e-mail domains except those in this table.

Whitelist

Registration is possible only via the e-mail domains that are present in this table.

Default:

Blacklist

2.24.41.1.9 Domain-list

With this list, you can specify whether you want e-mails from certain e-mail providers to be generally accepted or rejected. Use the "Add" button to add individual providers to the list. With the *2.24.41.1.8 Black-White-Domain-List* on page 919 you determine whether you accept or reject a provider.

Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.9.1 Domain

Using this entry you define the e-mail domains that you allow or prohibit in the case of logins by your Public Spot users via e-mail. With the *2.24.41.1.8 Black-White-Domain-List* on page 919 you determine whether you accept or reject a provider.

Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Domain-List**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.20 Real-Name

In this table, you can manage the different language variants for the sender's name used by the Public Spot module when sending login credentials via e-mail. If you do not specify any text for a language, the device automatically enters the internal default text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

2.24.41.1.20.1 Language

This parameter shows the language variant for the individual sender name.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Real-Name**

2.24.41.1.20.2 Contents

Use this parameter to set the sender name used for the selected language.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Real-Name**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.21 Body

In this table, you can manage the different language variants for the message text used by the Public Spot module when sending login credentials via e-mail. If you do not specify any text for a language, the device automatically enters the internal default text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.21.1 Language

This parameter shows the language variant for the individual message text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Body**

2.24.41.1.21.2 Contents

Use this parameter to set the message text used for the selected language. A range of variables and control characters are available. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user.

The following **variables** are available:

`$PSpotPasswd`

Placeholder for user-specific password for the Public Spot access.

`$PSpotLogoutLink`

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

The following **control characters** are available:

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Body**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.1.22 Subject

In this table, you can manage the different language variants for the subject line used by the Public Spot module when sending login credentials via e-mail. If you do not specify any text for a language, the device automatically enters the internal default text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

2.24.41.1.22.1 Language

This parameter shows the language variant for the individual subject-line text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Subject**

2.24.41.1.22.2 Contents

Use this parameter to set the subject line used for the selected language. The following control characters are available.

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Subject**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2 E-Mail2SMS-authentication

This menu specifies the settings for authentication to the network and transmission of the credentials. The latter is done by SMS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

2.24.41.2.1 Limit-e-mails-per-Hour

Enter the maximum number of e-mails sent within one hour to Public-Spot users with login data.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

Possible values:

Max. 5 characters from `[0-9]`

Default:

100

2.24.41.2.4 Max-Request-Attempts

With this parameter you specify how many different credentials can be requested for a MAC address within one day.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3

2.24.41.2.5 Local-e-mail-Address

Enter the sender e-mail address for the e-mail that is sent.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.13 Gateway-e-mail-Address

Here you enter the valid address of your e-mail2SMS gateway for sending the credentials via SMS message. Keep in mind any formatting specifications for the SMS gateway.

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PSpotUserMobileNr` for the user's mobile phone number

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.14 Allowed-Country-Codes

In this table you define the country codes that you allow in the case of a login by a Public Spot user via SMS (text message). A user can only have his login data sent to phone numbers with country codes that are included in this list.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

2.24.41.2.14.1 Name

Using this entry you assign a designation for the country code, for example, `DE` or `Germany`.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Allowed-Country-Codes**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.14.2 Code

Using this entry you assign the country code for the country that you want to add, for example, `0049` for Germany.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Allowed-Country-Codes**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.24.41.2.15 Send-SMS

This parameter specifies how the device sends SMS text messages. The choices available to you vary according to the device type.

In order to successfully send access credentials as a text message via a 3G/4G WWAN-enabled device, the device's internal SMS module must be set up under **Setup** > **SMS**.

SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Setup** > **Mail**.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

Possible values:

Send directly

The credentials are sent as an SMS text message via the 3G/4G WWAN module in this device.

HTTP2SMS

The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device

When registering with the Public Spot via SMS, you have the option of sending the access credentials via another device equipped with a 3G/4G WWAN module. To use this option, you must store the address and the access data for the other device on the device that provides the Public Spot. In order to send the SMS, the Public Spot module logs on to the other device and uses a URL to initiate the transmission of the text message via the 3G/4G WWAN module in the other device.

Make sure that the SMS module on the other device is configured correctly. In addition, we recommended that you create an administrator without access rights (select **None**) and with just one function right, **Send SMS**.

SMS gateway

The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

Default:

SMS gateway

2.24.41.2.16 HTTP-User-Name

With this parameter you specify the user name used by your device to authenticate at another device.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

Possible values:

Max. 16 characters from `[0-9][A-Z][a-z] @{|}~!$%&'()+-,/:;<=>?[\]^_.#*``

Default:

empty

2.24.41.2.17 HTTP-Password

With this parameter you specify the password for the user name used by your device to authenticate at another device.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

Possible values:

Max. 16 characters from `[0-9][A-Z][a-z] @{|}~!$%&'()+-,/:;<=>?[\]^_.#*``

Default:

empty

2.24.41.2.18 HTTP-Gateway-Address

This parameter specifies the IP address of the other device that is to be used for sending SMS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

Possible values:

Valid IPv4/IPv6 address, max. 15 characters from `[0-9][A-F][a-f]:./`

Default:

empty

2.24.41.2.19 SSL

This menu contains the parameters for the e-mail2Sms-Authentication.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

2.24.41.2.19.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.24.41.2.19.2 Keyex-Algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.24.41.2.19.3 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.24.41.2.19.4 Hash-Algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.24.41.2.19.5 Prefer-PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

No
Yes

Default:

Yes

2.24.41.2.19.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.24.41.2.19.7 Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.24.41.2.19.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.24.41.2.23 Real-Name

Using this entry you assign the country code for the country that you want to add, for example, `0049` for Germany.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

2.24.41.2.23.1 Language

This parameter shows the language variant for the individual sender name.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Real-Name**

2.24.41.2.23.2 Contents

Use this parameter to set the sender name used for the selected language.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Real-Name**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.24 Body

In this table, you can manage the different language variants for the message text used by the Public Spot module when sending login credentials via e-mail2SMS. If you do not specify any text for a language, the device automatically enters the internal default text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

2.24.41.2.24.1 Language

This parameter shows the language variant for the individual message text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Body**

2.24.41.2.24.2 Contents

Use this parameter to set the message text used for the selected language. A range of variables and control characters are available. The variables are automatically populated with values when the Public Spot module sends the e-mail to the SMS gateway.

The following **variables** are available:

`$PSpotPasswd`

Placeholder for user-specific password for the Public Spot access.

`$PSpotLogoutLink`

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

The following **control characters** are available:

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Body**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.25 Subject

In this table, you can manage the different language variants for the subject line used by the Public Spot module when sending login credentials via e-mail2SMS. If you do not specify any text for a language, the device automatically enters the internal default text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

2.24.41.2.25.1 Language

This parameter shows the language variant for the individual subject-line text.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Subject**

2.24.41.2.25.2 Contents

Use this parameter to set the subject line used for the selected language. The following control characters are available.

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Subject**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.2.26 Allowed-Prefixes

In this table you specify the permitted country codes for the option SmartTicket via SMS. Each country requires an entry in the Allowed-Country-Codes table.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

2.24.41.2.26.1 Country name

This is where you enter the name of the allowed country (e.g., Germany or DE) for which access to certain area dialing codes is to be restricted.

Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication** > **Allowed-Prefixes**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

Germany

2.24.41.2.26.2 Allowed country codes

Each country from the list Allowed-Country-Codes requires you to enter the allowed prefix(es) for the use of SmartTicket via SMS.

If you do not make an entry for a country in this table, all country codes will be allowed.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication** > **Allowed-Prefixes**

Possible values:

Max. 50 characters from `[0-9 , *]`

Default:

15*,16*,17*

2.24.41.3 User-Template

In this menu you manage the default values which the Public Spot uses to automatically create a user account if the login is made via e-mail, SMS (text message) or after confirming an agreement. The configurable parameters correspond closely to those of the setup wizard **Create Public Spot account**.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

2.24.41.3.2 Comment

Using this entry you specify a comment or informational text which the RADIUS server adds to an automatically created user account.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.3.3 Volume-Budget

With this entry you specify the volume budget in MBytes assigned to automatically created users. The value `0` deactivates the function.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

Max. 4 characters from `0123456789`

Default:

0

Special values:

0

switches off the monitoring of data volume.

2.24.41.3.4 Time-Budget

Using this entry you define the time budget which automatically created users are assigned.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

The value `0` deactivates the function.

2.24.41.3.5 Rel.-Expiry

Using this entry you define the relative expiry time of an automatically created user account (in seconds). The **Expiry-type** that you chose must include `relative` in order for this setting to work. The validity of the account terminates after the time period specified in this field from the time of the first successful login of the user.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

3600

2.24.41.3.6 Abs.-Expiry

Using this entry you define the absolute expiry time of an automatically created user account (in days). The **Expiry-type** that you chose must include `absolute` in order for this setting to work. The validity of the account terminates at the time specified in this field, calculated from the day of the creation of the account.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

365

2.24.41.3.7 Expiry-Type

Using this entry you define how an automatically created Public Spot user account expires. You can specify whether the validity period of a user account is absolute (e.g. expires on a set date) and/or relative (elapsed time since the first successful login). If you select both values, the expiry time depends on which case occurs first.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

Absolute
Relative

Default:

Absolute

Relative

2.24.41.3.8 Max-Concurrent-Logins

Using this entry you set the maximum number of devices which can concurrently login to an automatically created account. The value `0` stands for "unlimited".

In order for this setting to work, the parameter *2.24.41.3.9 Multiple-Login* on page 937 must be enabled.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

1

2.24.41.3.9 Multiple-Login

This entry allows you to generally allow or prohibit users with an automatically created account to login to the Public Spot using the same credentials with multiple devices at the same time. The number of devices that can be logged on simultaneously is specified using the parameter *2.24.41.3.8 Max-Concurrent-Logins* on page 937.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

No
Yes

Default:

Yes

2.24.41.3.10 Tx-Limit

With this setting you limit the maximum transmission bandwidth (in kbps), which is available to the user.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

The value 0 disables the limit (unlimited bandwidth).

2.24.41.3.11 Rx-Limit

With this setting you limit the maximum receiving bandwidth (in kbps), which is available to the user.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

0 … 4294967295

Default:

0

Special values:

0

The value 0 disables the limit (unlimited bandwidth).

2.24.41.3.12 Abs.-Expiry-Unit

Use this entry to set the units for the absolute expiry of the user template.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

Possible values:

Minute(s)

Specifies that the validity period is entered as minutes.

Hour(s)

Specifies that the validity period is entered as hours.

Day(s)

Specifies that the validity period is entered as days.

Default:

Day(s)

2.24.41.4 Login-via-agreement

In this menu, you specify the settings for automatic login and authentication via RADIUS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

2.24.41.4.1 Max-Request-per-Hour

This entry indicates the maximum number of users per hour, which can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

0 … 65535

Default:

100

2.24.41.4.2 User-Accounts-per-Day

This entry displays the number of accounts that a user can create on one day for the designated login mode. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot on the specified day.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

0 … 65535

Default:

1

2.24.41.4.3 Username-Prefix

This entry contains the prefix which is added to the automatically generated Public Spot username, when it is automatically generated by the device in the login mode "No Authentication" (automatic login and authentication).

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

free

2.24.41.4.4 Require-E-Mail

This entry allows you to specify whether the e-mail address of the user should be requested.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

No
Yes

Default:

No

2.24.41.4.5 Save-In-Min

This entry specifies the intervals at which user sessions are saved. The value is set in minutes.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

Max. 5 characters from `[0–9]`

Default:

1440

2.24.41.4.6 Mail-In-Min

This entry sets the interval (in minutes) before the list of collected users is sent to the specified e-mail address.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

0 … 65535

Default:

1440

2.24.41.4.7 E-Mail-List-Recipient

This entry contains the e-mail address to which the list of requested e-mail addresses is sent.

If you have already set the recipient e-mail address in LANconfig, it will be shown here.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.41.4.8 Unlock-Account-Creation

When the Public Spot module with the login method "Login after consent" is in use, the number of user accounts created for a requesting MAC address is stored for 24 hours. This is to enforce the limitation on the number of user accounts issued per MAC address.

This setting, once activated, means that the restriction on any particular MAC address is lifted not 24 hours after the creation of the user account(s), but instead daily at a specified time for all of the MAC addresses at once. The desired hour of the day (0-23) is entered under Unlock-Daily-On-Hr.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

No
Yes

Default:

No

2.24.41.4.9 Unlock-Daily-On-Hr

When the Public Spot module with the login method "Login after consent" is in use, the number of user accounts created for a requesting MAC address is stored for 24 hours. This is to enforce the limitation on the number of user accounts issued per MAC address.

If this was activated under Unlock-Account-Creation, the restriction on any particular MAC address is lifted not 24 hours after the creation of the user account(s), but instead daily at a specified time for all of the MAC addresses at once. The desired hour of the day (0-23) is entered here.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

0 … 23

2.24.41.5 Radius-Server

Use this menu to specify the settings used when Public Spot user accounts are created on the RADIUS server of the remote Public Spot gateway.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

2.24.41.5.1 Provider

Use this entry to specify the RADIUS server profile, which is located in the Public Spot provider table and references the RADIUS server of the remote Public Spot gateway.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.24.41.5.2 Name

Use this entry to specify which administrator account is used for creating user accounts on the remote Public Spot gateway.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.24.41.5.3 Password

Use this entry to enter the password for the administrator account specified above.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.24.41.5.4 SSL

This menu contains the parameters for the RADIUS server.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

2.24.41.5.4.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.24.41.5.4.2 Keyex-Algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.24.41.5.4.3 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.24.41.5.4.4 Hash-Algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.24.41.5.4.5 Prefer-PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

No
Yes

Default:

Yes

2.24.41.5.4.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.
Allowed
The device permits renegotiations with the remote station.
Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.24.41.5.4.7 Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server** > **SSL**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.24.41.5.4.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Authentication-Modules** > **SSL-for-Page-Table** > **Radius-Server** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
MD5-ECDSA
SHA1-ECDSA
SHA224-ECDSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.24.42 WISPr

This menu contains the WISPr settings.

Console path:

Setup > **Public-Spot-Module**

2.24.42.1 Operating

Enable or disable the WISPr function for your device.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

No
Yes

Default:

No

2.24.42.2 Location-ID

Use this ID to assign a unique location number or ID for your device, for example, in the format `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.3 Operator-name

Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.4 Location-name

Describe the location of your device, e.g., `CafeX_Market3`. This helps to better identify a user in your hotspot.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.5 Login-URL

Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.6 Logoff-URL

Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.7 Abort-Login-URL

Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.42.8 Max-Authen-Failure

Enter the maximum number of failed attempts which the login page of your Internet service provider allows.

Console path:

Setup > **Public-Spot-Module** > **WISPr**

Possible values:

0 … 65535

Default:

5

2.24.43 Advertisement

This menu gives you the option to enable or disable advertising pop-ups, and to edit these.

Console path:

Setup > **Public-Spot-Module**

2.24.43.1 Operating

This menu switches the advertisements on or off.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

Possible values:

No
Yes

Default:

No

2.24.43.2 Interval

This item allows you to specify the interval after which the Public Spot redirects a user to an advertisement URL.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

Possible values:

0 … 65535 Minutes

Default:

10

Special values:

0

Redirection takes place directly after signing on.

2.24.43.3 URL

This item is used to enter the advertisement URLs. If multiple URLs are entered, the Public Spot displays them in sequence after the specified interval.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

Possible values:

Max. 150 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.43.3.1 Contents

This parameter specifies the advertisement URL(s).

Console path:

Setup > **Public-Spot-Module** > **Advertisement** > **URL**

Possible values:

Max. 150 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.43.4 User-Agent-White-List

This item is used to add user agents which the Public Spot excludes from advertising.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

Possible values:

Max. 150 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.24.43.4.1 User-Agent

Name of the user agent you included in the white list.

Console path:

Setup > **Public-Spot-Module** > **Advertisement** > **User-Agent-White-List**

Possible values:

Max. 150 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.24.43.5 Process-WISPr-Redirect-URL

If the access-accept message from the RADIUS server contains the attribute 'WISPr-Redirection-URL', the Public Spot client is redirected to this URL after successful authentication. This scenario behaves in the same way as if the RADIUS server were to return 'LCS-Advertisement-URL=any' and 'LCS-Advertisement-Interval=0'. There is no need to set the **Operating** switch. The attribute 'WISPr-Redirection-URL' is sufficient. This configuration is useful if, after authentication (e.g. by MAC authentication), a client is to be redirected to a page just once.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

Possible values:

No
Yes

Default:

No

2.24.43.6 Free-Networks

This item is used to add networks which the Public Spot excludes from advertising.

Console path:

Setup > **Public-Spot-Module** > **Advertisement**

2.24.43.6.1 Host-Name

Enter the IP address of the additional network or server, which your Public Spot users are to be given advertisement-free access to.

Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow advertisement-free access to all of the subdomains of a particular domain. The entry `*.google.com` allows the addresses `mail.google.com`, and `maps.google.com`, etc.

Console path:

Setup > **Public-Spot-Module** > **Advertisement** > **Free-Networks**

Possible values:

Max. 64 characters from `[A-Z][0-9][a-z]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.43.6.2 Mask

Enter the netmask of the additional network or server, which your Public Spot users are to be given advertisement-free access to.

If you wish to authorize a domain or just a single workstation with the address named earlier, set `255.255.255.255` as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value `0.0.0.0`), the device ignores the table entry.

Console path:

Setup > **Public-Spot-Module** > **Advertisement** > **Free-Networks**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.24.44 Manage-User-Wizard

In this entry, you will find the advanced settings for the **Public Spot Manage Users** wizard.

Console path:

Setup > **Public-Spot-Module**

2.24.44.10 show-status-information

This entry gives you the option to hide status information in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

No

The Setup Wizard hides the following columns: **Online-Time**, **Traffic**, **Status**, **MAC-Address**, **IP-Address**.

Yes

The Setup Wizard displays all status information.

2.24.44.11 show-all-users-admin-independent

This entry allows you to display only those user accounts in the Setup Wizard that were created by the currently logged-in administrator.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard displays all Public Spot accounts.

No

The Setup Wizard only displays the Public Spot accounts created by the currently logged-on administrator.

Default:

Yes

2.24.44.12 show-expiry-typ

This entry gives you the option to hide the "Expiry type" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Expiry type" column.

No

The Setup Wizard hides the "Expiry type" column.

Default:

Yes

2.24.44.13 show-abs-expiry

This entry gives you the option to hide the "Absolute expiry" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Absolute expiry" column.

No

The Setup Wizard hides the "Absolute expiry" column.

Default:

Yes

2.24.44.14 show-rel-expiry

This entry gives you the option to hide the "Relative expiry" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Relative expiry" column.

No

The Setup Wizard hides the "Relative expiry" column.

Default:

Yes

2.24.44.15 show-time-budget

This entry gives you the option to hide the "Time budget" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Time budget" column.

No

The Setup Wizard hides the "Time budget" column.

Default:

Yes

2.24.44.16 show-volume-budget

This entry gives you the option to hide the "Volume budget MByte" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Volume budget MByte" column.

No

The Setup Wizard hides the "Volume budget MByte" column.

Default:

Yes

2.24.44.17 show-case-sensitive

This entry gives you the option to hide the "Case sensitive" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Case sensitive" column.

No

The Setup Wizard hides the "Case sensitive" column.

Default:

Yes

2.24.44.18 show-active

This entry gives you the option to hide the "Show active" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Show active" column.

No
The Setup Wizard hides the "Show active" column.

Default:

Yes

2.24.44.19 show-tx-limit

This entry gives you the option to hide the "TX limit" (max. transmission bandwidth) column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "TX limit" column.

No
The Setup Wizard hides the "TX limit" column.

Default:

Yes

2.24.44.20 show-rx-limit

This entry gives you the option to hide the "RX limit" (max. receiving bandwidth) column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "RX limit" column.

No
The Setup Wizard hides the "RX limit" column.

Default:

Yes

2.24.44.21 show-calling-station

This entry gives you the option to hide the "Show calling station" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Show calling station" column.

No

The Setup Wizard hides the "Show calling station" column.

Default:

Yes

2.24.44.22 show-called-station

This entry gives you the option to hide the "Show called station" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Show called station" column.

No

The Setup Wizard hides the "Show called station" column.

Default:

Yes

2.24.44.23 show-online-time

This entry gives you the option to hide the "Online time" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Online time" column.

No

The Setup Wizard hides the "Online time" column.

Default:

Yes

2.24.44.24 show-traffic

This entry gives you the option to hide the "Traffic (Rx / Tx Kbyte)" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Traffic (Rx / Tx Kbyte)" column.

No

The Setup Wizard hides the "Traffic (Rx / Tx Kbyte)" column.

Default:

Yes

2.24.44.25 show-status-column

This entry gives you the option to hide the "Status" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Status" column.

No

The Setup Wizard hides the "Status" column.

Default:

Yes

2.24.44.26 show-mac-address

This entry gives you the option to hide the "MAC address" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "MAC address" column.

No
The Setup Wizard hides the "MAC address" column.

Default:

Yes

2.24.44.27 show-ip-address

This entry gives you the option to hide the "IP address" column in the Setup Wizard.

Console path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "IP address" column.

No
The Setup Wizard hides the "IP address" column.

Default:

Yes

2.24.47 Check-Origin-VLAN

Use this parameter to specify whether the VLAN ID of the network where a user is authenticated is used by the XML interface to verify user requests. This is relevant, for example, in scenarios where several Public Spot SSIDs are separated by means of VLAN and a one-time authentication at one of these SSIDs should not automatically entitle the user to access the other SSIDs.

The parameter requires that you have also enabled the setup parameters 2.24.40.1 (the XML interface itself) and 2.24.40.2 (authentication by the XML interface via an internal or an external RADIUS server) .

Console path:

Setup > **Public-Spot-Module**

Possible values:

No
The Public Spot does not take the VLAN ID into account when verifying users. A one-time authentication entitles a user to access all of the SSIDs managed by the Public Spot. As long as the user account is valid, authentication is automatic.

Yes

The Public Spot takes the VLAN ID into account when verifying users. The Public Spot stores the VLAN ID to the column of the same name in the station table, assuming that the authentication by the RADIUS server was successful. This VLAN ID is the value for `SOURCE_VLAN` in the login request from the external gateway. If the Public Spot user moves to a network with a different VLAN ID, the Public Spot updates their station-table entry to "unauthenticated" and prompts the user to authenticate at the RADIUS server again. In this case, the user receives the sign-in page to authenticate again.

To learn more about the request and response types, as well as the `SOURCE_VLAN` element, refer to the Reference Manual.

Default:

No

2.24.48 Circuit-IDs

When a user authenticates at a Public Spot, the circuit ID configured in this table is an additional identifier sent by the AP to the WLC along with the user name and password.

When you create a new Public Spot account, the Public Spot setup wizard checks to see whether this table contains an entry for the logged-in administrator. If this is the case, the setup wizard inserts the circuit ID into the RADIUS user table as the "called station".

Console path:

Setup > **Public Spot**

2.24.48.1 Administrator

Contains the name of the administrator who is entitled to assign this circuit ID.

Console path:

Setup > **Public-Spot** > **Circuit-IDs**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/;<=>?[\]^_.`

Default:

empty

2.24.48.2 Circuit-ID

Contains the circuit ID sent by the AP to the WLC as an additional identifier along with the user name and password when a user authenticates at a Public Spot.

Console path:

Setup > **Public-Spot** > **Circuit-IDs**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.24.49 Brute-Force-Protection

This menu contains the settings for the brute-force protection used by the Public Spot.

Console path:

Setup > **Public-Spot-Module**

2.24.49.1 Max-Login-Tries

Specify how many unsuccessful attempts are permitted before the login block takes effect.

Console path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 3 characters from `[0-9]`

Default:

10

2.24.49.2 Blocking-Time-In-Minute

Specify how long the login block of the brute-force protection applies.

Console path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

2.24.49.3 Unblocking-Check-In-Second

Specify the interval after which the AP checks for the expiry of a login block for a MAC address.

Console path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

2.24.49.4 Unblock

Use this action to remove the login block on a MAC address. Enter the parameters as one or more space-separated MAC addresses.

MAC addresses are specified in the format `11:22:33:44:55:66`, `11-22-33-44-55-66` or `112233445566`.

Console path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

2.24.50 Auto-Re-Login

Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) In these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

With automatic re-login, the user only has be identified on the Public Spot the first time that they are within the cell. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.

Please note that authentication only takes place using the MAC address when auto-re-login is enabled.

In this menu you configure the parameters for automatic re-login.

Console path:

Setup > **Public-Spot-Module**

2.24.50.1 Operating

Enable or disable the automatic re-login with this action.

The authentication is only performed on the MAC address of the WLAN client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

Console path:

Setup > **Public-Spot-Module** > **Auto-Re-Login**

Possible values:

No
Yes

Default:

No

2.24.50.2 Station-Table-Limit

You can increase the maximum number of clients that are allowed to use the re-login function to up to 65,536 participants.

While the device is operating, the only changes to the station table that take immediate effect are the additions to it. Restart the access point in order to immediately reduce the size of the station table.

Console path:

Setup > **Public-Spot-Module** > **Auto-Re-Login**

Possible values:

16 … 65536

Default:

8192

2.24.50.3 Exist-Timeout

This value indicates how long the Public Spot stores the credentials in the table of a WLAN client for a re-login. After this period (in seconds) has expired, the Public Spot user must log in again using the login page of the Public Spot in the browser.

If a Public Spot user has a time quota that is smaller than the timeout interval set here, this parameter has no effect. An automatic re-login does not occur if the user has the status "unauthenticated".

Console path:

Setup > **Public-Spot-Module** > **Auto-Re-Login**

Possible values:

Max. 10 characters from `[0-9]`

Default:

259200

2.24.51 Redirect-TLS-connections

Use this option to determine whether the Public Spot redirects HTTPS connections for unauthenticated clients. With this option disabled, unauthenticated clients are unable to establish HTTPS connections.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No

The Public Spot does not perform HTTPS redirects for unauthenticated WLAN clients.

Yes

The Public Spot performs HTTPS redirects for unauthenticated WLAN clients.

Default:

No

2.24.52 Monitor-Capacity

This menu contains the configuration options for the monitoring of the Public Spot module.

Console path:

Setup > **Public-Spot-Module**

2.24.52.1 Warning

Specifies whether the monitoring issues warnings.

Console path:

Setup > **Public-Spot-Module** > **Monitor-Capacity**

Possible values:

No
Yes

Default:

Yes

2.24.52.2 E-mail

This entry contains the e-mail address to which the monitoring sends the warnings.

Console path:

Setup > **Public-Spot-Module** > **Monitor-Capacity**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.53 SSL-for-Page-Table

This menu contains the parameters for the page table.

Console path:

Setup > **Public-Spot-Module**

2.24.53.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.24.53.2 Keyex-Algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.24.53.3 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

2.24.53.4 Hash-Algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

SHA1

SHA2-256

SHA2-384

2.24.53.5 Prefer-PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

No
Yes

Default:

Yes

2.24.53.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.24.53.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Public-Spot-Module** > **Authentication-Module** > **SSL-for-Page-Table**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.24.53.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Public-Spot-Module** > **SSL-for-Page-Table**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
MD5-ECDSA
SHA1-ECDSA
SHA224-ECDSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.24.55 Accept-CoA

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

With this entry you enable or disable the dynamic authorization of Public Spot users by means of RADIUS CoA via an external hotspot gateway.

Console path:

Setup > **Public-Spot-Module**

Possible values:

No

Dynamic authorization disabled. If there is a change to the RADIUS connection attributes, authorized users remain unaffected until their session expires.

Yes

Dynamic authorization enabled. The external gateway is able to modify the connection attributes of authorized users, or to disconnect existing sessions.

Default:

No

2.24.60 Login-Text

Use this table to manage the login texts.

The Public Spot module gives you the option to specify customized text, which appears on the login page inside the box of the login form. This **Login text** can be stored in multiple languages. The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text is specified for a language, then the device falls back to the English login text (if available).

Console path:

Setup > **Public-Spot-Module**

2.24.60.1 Language

This parameter shows the language of the login text to be entered.

Console path:

Setup > **Public-Spot-Module** > **Login-Text**

2.24.60.2 Contents

Use this parameter to set the login text used for the selected language. To type umlauts, you should use their HTML equivalents (such as `&uuml;` for ü), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text.

Example

```
Welcome!<br/><i>Please complete this form.</i>)
```

Console path:

Setup > **Public-Spot-Module** > **Login-Text**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.61 Login-Instructions

This menu is used to set a login title for your Public Spot page. You can define the title in six languages (English, German, French, Italian, Spanish and Dutch).

Console path:

Setup > **Public-Spot-Module**

2.24.61.1 Language

This entry displays the language selected for the login title.

Console path:

Setup > **Public-Spot-Module** > **Login-Instructions**

2.24.61.1 Contents

Enter the login title for your Public Spot here.

Console path:

Setup > **Public-Spot-Module** > **Login-Instructions**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.24.62 MAC-Address-Username-Format

With the login method "Authenticate with name, password and MAC address", the MAC address of the Public Spot client can be checked by an external RADIUS server. The format used to transmit the MAC address to the RADIUS server can be set here.

The individual bytes of the MAC address are represented here as the variables %a to %f. In the default setting specified here (%a%b%c-%d%e%f), the bytes of the MAC address are output one after the other with "-" as the separator. In addition to these variables, any of the characters supported by LCOS can be added.

Console path:

Setup > **Public-Spot-Module**

Possible values:

Max. 30 characters from `[]A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

%a%b%c-%d%e%f

2.24.63 Api-Server

The Public Spot supports the new Captive Portal API standard according to *RFC 8908*. The standard allows Wi-Fi clients in a hotspot to automatically find a captive portal or login page.

The client receives the URL of the portal page via DHCP and uses an API request to the hotspot to check whether a login is required or whether access is already permitted for the client. This significantly speeds up the user experience in a hotspot and, by defining a standard, now provides better manufacturer interoperability between hotspots and clients.

The following steps are required:

1. The use of TLS certificates in the Public Spot is mandatory. Without an HTTPS login, the client does not send a request to the portal.
2. The DHCP server must provide the Captive Portal DHCP option to the client.

Console path:

Setup > **Public-Spot-Module**

2.24.63.1 Operating

Enables or disables the Captive Portal API function in the Public Spot.

Console path:

Setup > **Public-Spot-Module** > **Api-Server**

Possible values:

No
Yes

Default:

No

2.24.63.2 User-Portal-URL

(Optional) By default, the Captive Portal API supports TLS only. For this reason the device must have a trusted certificate and a DNS name. By default, the parameter can be left empty and it will be inserted automatically by the system. To do this, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate. If an external hotspot server is used, a URL of this server can be entered here. Another requirement is that the clients in the hotspot must find the captive portal via DHCP option. For this purpose, the corresponding DHCP option according to *RFC 8910* must be configured for the hotspot network.

Console path:

Setup > **Public-Spot-Module** > **Api-Server**

Possible values:

Max. 251 characters from `[]A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.24.63.3 Venue-Info-URL

(Optional) URL (TLS) through which the operator can provide the user with additional information about the location of the hotspot, e.g. the website of the hotel with the hotspot.

Console path:

Setup > **Public-Spot-Module** > **Api-Server**

Possible values:

Max. 251 characters from `[]A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.25 RADIUS

This menu contains the settings for the RADIUS server.

Console path:

Setup

2.25.4 Auth.-Timeout

This value specifies how many milliseconds should elapse before retrying RADIUS authentication.

Console path:

Setup > **RADIUS**

Possible values:

Max. 10 characters from `[0-9]`

Default:

5000

2.25.5 Auth.-Retry

This value specifies how many authentication attempts are made in total before a Reject is issued.

Console path:

Setup > **RADIUS**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.25.9 Backup-Query-Strategy

This value specifies how the device should handle unanswered queries from multiple RADIUS servers.

Console path:

Setup > **RADIUS**

Possible values:

Block

The device first returns the maximum number of repeat queries to the first server before forwarding them to the backup server.

Cyclic

The device sends unanswered queries to the configured servers by turns.

Default:

Block

2.25.10 Server

This menu contains the settings for the RADIUS server.

Console path:

Setup > **RADIUS**

2.25.10.1 Authentication port

Specify here the port used by the authenticators to communicate with the RADIUS server in the access point.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

Switches the RADIUS server off.

2.25.10.2 Clients

Here you enter the clients that are to communicate with the RADIUS server.

Console path:

Setup > **RADIUS** > **Server**

2.25.10.2.1 IP network

IP network (IP address range) of RADIUS clients for which the password defined in this entry applies.

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

Special values:

0

Switches the RADIUS server off.

2.25.10.2.2 Secret

Password required by the client for access to the RADIUS server in the access point.

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.2.3 IP-Netmask

IP netmask of the RADIUS client

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.25.10.2.4 Protocol

Protocol for communication between the internal RADIUS server and the clients.

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

RADSEC
RADIUS
all

Default:

RADIUS

2.25.10.2.5 Comment

Comment on this entry.

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.2.6 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Proxy-Only
If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No

2.25.10.3 Forward-Servers

If you wish to use RADIUS forwarding, you have to specify further settings here.

Console path:

Setup > **RADIUS** > **Server**

2.25.10.3.1 Realm

String with which the RADIUS server identifies the forwarding destination.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.3.3 Port

Open port for communications with the forwarding server.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.25.10.3.4 Secret

Password required for accessing the forwarding server.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.3.5 Backup

Alternative routing server that the RADIUS server forwards requests to when the first routing server is not reachable.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.3.6 Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If the list of IP networks or loopback addresses contains an entry named "DMZ", the associated IP address will be used.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.

2.25.10.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

RADSEC
RADIUS

Default:

RADIUS

2.25.10.3.9 Accnt.-Port

Enter the port of the server to which the integrated RADIUS server forwards data packets for accounting.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

0 … 65535

Default:

0

2.25.10.3.10 Accnt.-Secret

Enter the valid shared secret for access to the accounting server here. Ensure that this key is consistent with that in the accounting server.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.3.11 Accnt.-Loopback-Adresse

Optionally enter a different address here (name or IP) to which the RADIUS forwarding accounting server sends its reply message.

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Name of the IP network (ARF network), whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If an interface with the name "DMZ" already exists, the device will select that address instead.

LB0 … LBF for one of the 16 loopback addresses or its name.
Any IPv4 address.

2.25.10.3.12 Accnt.-Protocol

Using this item you specify the protocol that the forwarding accounting server uses.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

RADSEC
RADIUS

Default:

RADIUS

2.25.10.3.13 Host name

Here you enter the IP address (IPv4, IPv6) or hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

2.25.10.3.14 Host name

Here you enter the IP address (IPv4, IPv6) or hostname of the RADIUS server to which the RADIUS client forwards the accounting data packets.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

2.25.10.3.15 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.10.3.16 Accnt.-Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.10.3.18 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

2.25.10.5 Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.25.10.6 Empty realm

This realm is used when the specified username does not contain a realm.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.25.10.7 User name

In the following table, enter the data for the users that are to be authenticated by this server.

Console path:

Setup > **RADIUS** > **Server**

2.25.10.7.1 User name

User name.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.7.2 Password

User password.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.7.3 Limited-Auth-Methods

This option allows you to place limitations on the authentication methods permitted for the user.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

PAP
CHAP
MSCHAP
MSCHAPv2
EAP
All

Default:

All

2.25.10.7.4 VLAN-ID

Using this input field you assign the user an individual VLAN ID. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value `0` disables the assignment of an individual VLAN ID.

For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server – in the setup menu **Setup** > **DHCP** – as short as possible. Possible values (in minutes) include, for example:

Max. lease time minutes

2

Default lease time minutes

1

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using a different DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

0 … 4094

Default:

4

2.25.10.7.5 Calling-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs. The ID is sent by the calling station (WLAN client). During the authentication by 802.1X, the MAC address of the calling station is transmitted in ASCII format (uppercase only). Each pair of characters is separated by a hyphen (e.g. `00-10-A4-23-19-C0`).

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 64 characters `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Special values:

*****

The wildcard `*` can be used to include whole groups of IDs to act as a mask.

Default:

empty

2.25.10.7.6 Called-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs. The ID is sent by the called station (BSSID and SSID of the AP). During the authentication by 802.1X, the MAC address (BSSID) of the called station is transmitted in ASCII format (uppercase only). Each pair of characters is separated by a hyphen; the SSID is appended after a separator, a colon (e.g. `00-10-A4-23-19-C0:AP1`).

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 64 characters `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Special values:

*****

The wildcard `*` can be used to include whole groups of IDs to act as a mask.

With the mask `*:AP1*`, for example, you define an entry that applies to a client in the radio cell with the name `AP1`, irrespective of which AP the client associates with. This allows the client to switch (roam) from one AP to the next while always using the same authentication data.

Default:

empty

2.25.10.7.7 Tx-Limit

Limitation of bandwidth for RADIUS clients.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

0 … 4294967295

Default:

0

2.25.10.7.8 Rx-Limit

Limitation of bandwidth for RADIUS clients.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

0 … 4294967295

Default:

0

2.25.10.7.9 Multiple logins

Allows or prohibits more than one parallel session with the same user ID. If parallel sessions are prohibited, the device rejects authentication requests for a user ID for which a session is already running in the active session accounting table. This is a prerequisite to enforce time and volume budgets.

The multiple-login option must be deactivated if the RADIUS server is to monitor a time budget. The time budget can only be monitored if the user is running just one session at a time.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

No
Yes

Default:

Yes

2.25.10.7.10 Abs.-Expiry

If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 20 characters from `[0-9]/:.`

Default:

0

Special values:

0

The value "0" switches off the monitoring of the absolute expiry time.

2.25.10.7.11 Time budget

The maximum duration of access time for this user account, in seconds. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" switches off the monitoring of the absolute expiry time.

2.25.10.7.13 Expiry type

This option defines how the validity period is limited for a user account.

The device must have a valid time in order for the device to work with user-account time budgets.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Absolute

The validity of the user account terminates at a set time.

Relative

The validity of the user account terminates a certain period of time after the first user login.

none

The user account never expires, unless a predefined time or volume budget expires.

Default:

Absolute

2.25.10.7.14 Rel.-Expiry

If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" switches off the monitoring of the relative expiry time.

2.25.10.7.15 Comment

Comment on this entry.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.7.16 Service type

The service type is a special attribute of the RADIUS protocol. The NAS (Network Access Server) sends this with the authentication request. The response to this request is only positive if the requested service type agrees with the user account service type. For example, the service type for Public Spot is "Login" and for 802.1x "Framed".

The number of entries permissible with the service type "any" or "login" is 64 or 256, depending on the model. This means that the table is not completely filled with entries for Public Spot access accounts (using the service type "Any") and it enables the parallel use of logins via 802.1x.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Any

Framed

For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.

Login

For Public Spot authentications.

Authorize only

For RADIUS authentication of dialup peers via PPP.

Default:

Any

2.25.10.7.17 Case sensitive

This setting specifies whether the RADIUS server handles the user name case-sensitive.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

No
Yes

Default:

Yes

2.25.10.7.18 WPA passphrase

Here you can specify the WPA passphrase with which users can login to the WLAN.

The RADIUS server stores this passphrase in the user table. This enables a device which is connected to the LAN to operate as a central RADIUS server and use the benefits of LEPS (LANCOM Enhanced Passphrase Security).

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

8 … 63 ASCII character set

Default:

empty

2.25.10.7.19 Max-Concurrent-Logins

If you have enabled multiple logins, this parameter specifies how many clients can be concurrently logged in to this user account.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

8 … 4294967295

Default:

0

2.25.10.7.20 Operating

Using this parameter, you specifically enable or disable individual RADIUS user accounts. This makes it possible, for example, to disable individual accounts temporarily without deleting the entire account.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

No
Yes

Default:

Yes

2.25.10.7.21 Shell-Priv.-Level

This field contains a vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

0 … 4294967295

Default:

0

2.25.10.7.22 Volume budget MByte

This entry enables you to set the budget volume of the RADIUS user in megabytes.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The volume budget is deactivated.

2.25.10.7.23 Tunnel-Password

This entry sets the connection password for each user.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.10.7.24 LCS-Routing-Tag

Specify the routing tag for this connection.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.25.10.7.25 Attribute-Values

User-defined attributes for RADIUS users in the RADIUS server.

Along with the user-management attributes supported by the LANCOM RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users here.

Console path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Semicolon-separated list of attributes and values in the form
<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2> ...

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.10.10 EAP

This menu contains the EAP settings.

Console path:

Setup > **RADIUS** > **Server**

2.25.10.10.1 Tunnel server

This realm refers to the entry in the table of the forwarding server that is to be used for tunneled TTLS or PEAP requests.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

Max. 24 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.3 Reauth period

When the internal RADIUS server responds to a client request with a CHALLENGE (negotiation of authentication method not yet completed), the RADIUS server can inform the authenticator how long it should wait (in seconds) for a response from the client before issuing a new CHALLENGE.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

No timeout is sent to the authenticator.

The function is not supported by all authenticators.

2.25.10.10.4 Retransmit timeout

When the internal RADIUS server responds to a client request with an ACCEPT (negotiation of authentication method completed successfully), the RADIUS server can inform the authenticator how long it should wait (in seconds) before triggering repeat authentication of the client.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

No timeout is sent to the authenticator.

The function is not supported by all authenticators.

2.25.10.10.5 TTLS-Default-Tunnel-Method

Two authentication methods are negotiated when TTLS is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

None
MD5
GTC
MSCHAPv2

Default:

MD5

2.25.10.10.6 PEAP-Default-Tunnel-Method

Two authentication methods are negotiated when PEAP is used. A secure TLS tunnel is first negotiated using EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). The the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

None
MD5
GTC
MSCHAPv2

Default:

MSCHAPv2

2.25.10.10.7 Default-Method

This value specifies which method the RADIUS server should offer to the client outside of a possible TTLS/PEAP tunnel.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

None
MD5
GTC
MSCHAPv2
TLS
TTLS
PEAP
WFA-Unauth
OTP

Default:

MD5

2.25.10.10.8 Default MTU

Define the Maximum Transmission Unit to be used by the device as the default for EAP connections.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

100 … 1496 Bytes

Default:

1036

2.25.10.10.9 Allowed methods

Here you select the server and the method for the EAP authentication.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

2.25.10.10.9.1 Method

Select the default EAP authentication method.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **Allow-Methods**

Possible values:

None
MD5
GTC
MSCHAPv2
TLS
TTLS
PEAP
WFA-Unauth

This method only needs to be enabled when using the RADIUS server in the LCOS for an encrypted OSU SSID.

Default:

MD5

GTC

MSCHAPv2

TLS

TTLS

PEAP

2.25.10.10.9.2 Allow EAP-TLS

Enable the EAP-TLS method for authentication here.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **Allow-Methods**

Possible values:

No
Yes
Internal only

Default:

Yes

2.25.10.10.10 MSCHAPv2-Backend-Server

This setting lets you define an optional external RADIUS server to be used by the internal RADIUS server operating EAP-MSCHAPv2 (as is usual for example in a PEAP tunnel) to outsource the MS-CHAP v2 response check. This enable you to outsource the user database to an external RADIUS server that does not support EAP.

Note that the external RADIUS server must support at least MSCHAPv2 because CHAP leaves the actual password on the server.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.19 EAP-TLS

The parameters for EAP-TLS connections are specified here.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

2.25.10.10.19.2 Versions

Specify which TLS version(s) are to be used for the Extensible Authentication Protocol (EAP).

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

TLSv1
TLSv1.1
TLSv1.2

Default:

TLSv1

2.25.10.10.19.3 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.25.10.10.19.4 Crypro algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.25.10.10.19.5 Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.25.10.10.19.6 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

On
Off

Default:

On

2.25.10.10.19.8 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.25.10.10.19.10 Check-Username

TLS authenticates the client via certificate only. If this option is activated, the RADIUS server additionally checks if the username in the certificate is contained in the RADIUS user table.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

Yes
No

Default:

No

2.25.10.10.19.22 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.25.10.10.20 EAP-OTP

The parameters for EAP-OTP are set here.

Console path:

Setup > **RADIUS** > **Server** > **EAP**

2.25.10.10.20.1 Users

In this table the OTP users are defined.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP**

2.25.10.10.20.1.1 User-Name

Enter the name of the OTP user here. This must already be contained in the RADIUS user accounts table with the same name.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.20.1.2 Calling-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs transmitted by the calling station.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.20.1.3 Called-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs transmitted by the called station.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.20.1.4 Hash-Algorithm

Defines the hash algorithm used.

Note that the Authenticator app supports the maximum possible hash algorithm. For example, Google Authenticator currently supports only SHA1 on certain Android platforms.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

SHA1
SHA256
SHA512

Default:

SHA1

2.25.10.10.20.1.5 Time-Step

Defines the interval in seconds after which a new OTP is calculated.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

2.25.10.10.20.1.6 Network-Delay

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 3 characters from `[0-9]`

2.25.10.10.20.1.7 Secret

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Base32 (Default)

Prefix “base32:” followed by the base32 encoded secret. The prefix “base32:” may also be omitted.

Hexadecimal

Prefix “hex:” followed by an even number of hex digits.

Plain text passphrase

Prefix “ascii:” and then the characters.

For Google Authenticator, the secret must be 16 characters long (80 bit, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.10.20.1.8 Num-Digits

Length of the OTPs.

For Google Authenticator, the value 6 should be used.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 3 characters from `[0-9]`

Default:

6

2.25.10.10.20.1.9 Issuer

Freely definable text used in Authenticator to keep multiple keys apart when the same username is used. Must not contain a colon.

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.11 Accounting port

Enter the port used by the RADIUS server to receive accounting information. Port '1813' is normally used.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

Special values:

0

Switches the use of this function off.

2.25.10.12 Accounting Interim Interval

Enter the value that the RADIUS server should output as "Accounting interim interval" after successful authentication. Provided the requesting device supports this attribute, this value determines the intervals (in seconds) at which an update of the accounting data is sent to the RADIUS server.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

60 … 4294967295

Default:

0

Special values:

0

Switches the use of this function off.

2.25.10.13 RADSEC port

Enter the (TCP) port used by the server to accept accounting or authentication requests encrypted using RADSEC. Port 2083 is normally used.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

Deactivates RADSEC in the RADIUS server.

2.25.10.14 Auto-Cleanup-User-Table

With this feature enabled, the RADIUS server automatically deletes accounts from the Users table when the expiry date has passed.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

No
Yes

Default:

No

2.25.10.15 Allow-Status-Requests

Here you specify whether to allow status requests.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

No
Yes

Default:

No

2.25.10.16 IPv6 clients

Here you specify the RADIUS access data for IPv6 clients.

Console path:

Setup > **RADIUS** > **Server**

2.25.10.16.1 Address-Prefix-Length

This value specifies the IPv6 network and the prefix length, e.g., "fd00::/64". The entry "fd00::/64", for example, permits access to the entire network, the entry "fd00::1/128" only permits exactly one client.

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

2.25.10.16.2 Address-Prefix-Length

This value specifies the password required by the clients for access to the internal server.

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

Max. 43 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.10.16.4 Protocols

This selection specifies the protocol for communication between the internal server and the clients.

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

RADIUS
RADSEC
All

Default:

RADIUS

2.25.10.16.5 Comment

Comment on this entry.

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.10.16.6 Require-Msg-Authenticator

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Proxy-Only
If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No

2.25.10.17 Realm types

Specify how the RADIUS server determines the realm of a RADIUS request.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Mail domain

`user@company.com`: `company.com` is the realm and is separated from the name of the user by an @ character.

MS domain

`company\user`: `company` is the realm and is separated from the name of the user by a backslash ("\"). This form of authentication is used for a Windows login, for example.

MS-CompAuth

`host/user.company.com`: If the user name starts with the string `host/` and the rest of the name contains at least one dot/period, the device considers everything after the first dot to be the realm (in this case `company.com`).

Default:

Mail domain

MS domain

2.25.10.18 Auto-Cleanup-Accounting-Totals

This entry gives you the option of deleting all of the access information on the RADIUS server.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

No

Accouting information is not automatically deleted.

Yes

Accounting information is deleted automatically.

Default:

No

2.25.10.19 Allow multi-login

Specifies whether multiple logins are allowed.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

None
Multiple logins are not allowed.

Same-Calling-Station-Id
Multiple logins are allowed for devices with the same calling-station ID.

Default:

None

2.25.10.21 Authentication operating

Enable/disable the authentication here.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Yes
No

Default:

No

2.25.10.22 IPv4-WAN-Access

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

No
The RADIUS server rejects WAN traffic from the IPv4 network.

Yes
The RADIUS server accepts WAN traffic from the IPv4 network.

VPN
The RADIUS server accepts only WAN traffic from the IPv4 network that arrives at the device over a VPN connection.

Default:

No

2.25.10.31 Accounting operating

Enable/disable the accounting here.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Yes
No

Default:

No

2.25.10.33 RADSEC operating

Here you enable/disable **RADSEC**.

Console path:

Setup > **RADIUS** > **Server**

Possible values:

Yes
No

Default:

No

2.25.19 Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176*.

Console path:

Setup > **RADIUS**

2.25.19.1 Operating

This entry enables or disables the dynamic authorization by RADIUS.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

2.25.19.2 Port

This entry specifies the port on which CoA messages are accepted.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3799

2.25.19.3 WAN access

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

2.25.19.4 Clients

All of the CoA clients that send messages to the NAS are entered into this table.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

2.25.19.4.1 HostName

This entry contains the unique identifier of the client that sends messages to the NAS.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.19.4.2 Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.19.5 Forward-Servers

To forward CoA messages, the forwarding servers are specified here.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

2.25.19.5.1 Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.19.5.2 HostName

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.19.5.3 Port

This entry contains the port for communications with the forwarding server.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.25.19.5.4 Secret

This entry specifies the secret required to access the forwarding server.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.19.5.5 Loopback

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

Console path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.25.19.6 Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.25.19.7 Empty realm

This realm is used when the specified username does not contain a realm.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.25.19.8 Radclient

Use the command `do Radclient [...]` to send CoA messages.

The Radclient command is structured as follows:

```
do Radclient <server[:port]> coa/disconnect <secret> <attribute-list>
```

Outputs all known and active RADIUS sessions

Entering the command `show dynauth sessions` on the command line lists the RADIUS sessions that are known to the CoA module. This outputs the session reported by the Public Spot module. The known attributes for this session are shown in the section "Context":

```
Session with MAC-Address: [a3:18:22:0c:ae:df] Context: [NAS-IP-Address:
192.168.1.254,User-Name:  user46909,  NAS-Port-Id:  WLC-TUNNEL-1,
Framed-IP-Address: 192.168.1.78]
```

The attributes "NAS-IP-Address" and "Username" identify the active session. If you wish to limit the bandwidth for the active session, you enter the Radclient command with these values along with the attributes "LCS-TxRateLimit" and "LCS-RxRateLimit" in combination with the transmission and reception limits in kbps:

```
do Radclient 192.168.1.254 coa secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254;LCS-TxRateLimit=5000;LCS-RxRateLimit=5000"
```

Note that the identification attributes and the attributes being modified must be specified with the same rights in the attribute list.

Terminate an active RADIUS session

A running RADIUS session is terminated by using the Radclient command to send a disconnect message:

```
do Radclient 192.168.1.254 disconnect secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254"
```

The Radclient command integrated in LCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

Console path:

Setup > **RADIUS** > **Dyn-Auth**

2.25.20 RADSEC

The parameters for READSEC connections are specified here.

Console path:

Setup > **RADIUS**

2.25.20.1 Versions

This bitmask specifies which versions of the protocol are allowed.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default:

SSLv3

TLSv1

2.25.20.2 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.25.20.3 Crypro-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.25.20.4 Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.25.20.5 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

On
Off

Default:

On

2.25.20.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.25.20.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.25.20.21 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **RADIUS** > **RADSEC**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.25.21 Availability monitoring

In this directory you configure the availability monitoring.

Monitoring is performed by sending status server requests or access requests.

Console path:

Setup > **RADIUS**

2.25.21.1 Profiles

Here you create monitoring profiles for the availability of RADIUS servers.

Console path:

Setup > **RADIUS** > **Supervision-Servers**

2.25.21.1.1 Name

Enter the name of the availability monitoring profile here.

Console path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

DEFAULT

2.25.21.1.2 Type

Here, you specify whether status server or access requests are sent to the RADIUS server for the purpose of availability monitoring.

Console path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Access request
Status server

Default:

Access request

2.25.21.1.3 Attributes

If availability monitoring is performed with access requests, you can specify the attributes of the access request here by means of a comma-separated list in the format **Attribute1=value1,Attribute2=value2, etc.**. Accessibility checks by means of an access request require at least the specification of the attribute "User-Name", e.g. **User-Name=dummyuser**.

Status server requests do not require any attributes.

Console path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.25.21.1.4 Request interval

Here you define the interval in seconds used by the RADIUS server to check the availability.

Console path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

`[0-9]`

Default:

60

2.25.22 User-Defined-Attributes

This directory is for user-defined attributes.

RADIUS attributes are managed in what is known as a dictionary. LCOS supports many different attributes by default; however, there is a huge variety of manufacturer-specific attributes, which the administrator can enter into the LCOS configuration here. These attributes can then be used in the LCOS at any point where attributes can be added to a RADIUS request or response, e.g. in the RADIUS user management.

Console path:

Setup > **RADIUS**

2.25.22.1 Attributes

Here you create the user-defined attributes for use with RADIUS servers.

Console path:

Setup > **RADIUS** > **User-Defined-Attributes**

2.25.22.1.1 Name

The name used to reference the attribute in other places in LCOS.

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]-_`

2.25.22.1.2 Vendor-ID

The specific vendor ID of the attribute.

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Max. 10 characters from `[0-9]`

2.25.22.1.3 Vendor-Type

The specific type ID of the attribute.

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Max. 3 characters from `[0-9]`

2.25.22.1.4 Data-Type

The specific type ID of the attribute.

Console path:

Setup > **RADIUS** > **User-Defined-Attributes** > **Attributes**

Possible values:

Text
Integer
IPv4-Address
IPv6-Address
Date

2.25.23 Dynamic-Peer-Discovery

Support for *RFC 7585* "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)". Instead of statically forwarding RADIUS requests to one or more RADIUS servers, Dynamic Peer Discovery dynamically finds the correct RADIUS server based on the realm/NAI. If a request arrives, the correct server is found via DNS NAPTR/SRV record.

Console path:

Setup > **RADIUS**

2.25.23.1 Operating

Switch Dynamic Peer Discovery on or off. As soon as Dynamic Peer Discovery is enabled, the RADIUS server branches to dynamic resolution if a specific realm is not defined in its forwarding table. dynamic resolution if a particular realm/NAI is not defined in its forwarding table. Local definitions for realms always have priority.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

No
Yes

Default:

No

2.25.23.2 Routing-Tag

The routing tag that Dynamic Peer Discovery should use for its DNS queries.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.25.23.3 Loopback-Address

The loopback address to use when forwarding to RADIUS servers determined by Dynamic Peer Discovery.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.25.23.4 Attribute-Values

RADIUS attributes to be added or changed when forwarding to servers discovered by Dynamic Peer Discovery.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.25.23.5 Services

TTable with the services. The service is what is delivered in the NAPTR response in the service. All NAPTR entries are extracted and are extracted and further resolved, which have as service the one with the highest priority from this table. If the default setting, for example, NAPTR records for both service types are supplied, those for “x-eduroam:radius.tls” are ignored. The table is automatically sorted by the LCOS so that higher prioritized services are placed higher up. The protocol that must be used to such a server (RADIUS or RADSEC) is explicitly specified. In case the NAPTR request does not return any usable records, this table still has the meaning, which prefix is put in front of the NAI for the fallback SRV request. The highest priority entry is taken from the table for which a prefix is defined in an internally fixed table. Currently

the services radius.tls, radius.tls.tcp, radsec.tcp and radius.udp are defined, which respond to a prefix of _radiustls._tcp., _radsec.tcp. or _radius._udp. respectively.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

2.25.23.5.1 Priority

Priority of this service.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

Possible values:

Max. 10 characters from `[0-9]`

2.25.23.5.2 Service

The services themselves. The defaults are “aaa+auth:radius.tls.tcp” and “x-eduroam:radius.tls”.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

Possible values:

Max. 32 characters from `[A-Z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.25.23.5.3 Protocol

The protocol used for this service.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery** > **Services**

Possible values:

RADIUS
RADSEC

2.25.23.6 DNS-Timeout

The amount of time in seconds within which all DNS requests for an NAI must be handled. This also includes the two-step variant via NAPTR and subsequent SRV queries.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.25.23.7 Min.-Eff.-TTL

TTL values reported by the DNS server that are shorter than this time are raised to this value.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 10 characters from `[0-9]`

Default:

60

2.25.23.8 Backoff-Time

If a resolution ends in an error (DNS response with error, timeout…), this is the time in seconds for which no new resolution attempts should be made for this realm.

Console path:

Setup > **RADIUS** > **Dynamic-Peer-Discovery**

Possible values:

Max. 10 characters from `[0-9]`

Default:

600

2.26 NTP

This menu contains the NTP settings.

Console path:

Setup

2.26.3 BC-Mode

If the device should regularly operate as a time server and send the current time to all stations in the network, enable the “send mode” here.

The send mode of the device only supports IPv4 addresses.

Console path:

Setup > **NTP**

Possible values:

No

The send mode is disabled.

Yes

The send mode is enabled.

Default:

No

2.26.4 BC-Interval

Here you set the time interval after which your device's time server sends the current time to all devices or stations accessible via the local network.

Console path:

Setup > **NTP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

64

2.26.7 RQ-Interval

Specify the time interval in seconds after which the internal clock of the device is re-synchronized with the specified time server (NTP).

A connection may be established in order to access the time server. Please be aware that this may give rise to additional costs.

Console path:

Setup > **NTP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

86400

2.26.11 RQ-Address

Here you enter the time server that supplies the correct current time.

Console path:

Setup > **NTP**

2.26.11.1 RQ-Address

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.

Console path:

Setup > **NTP** > **RQ-Address**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.26.11.2 Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- Name of the IP network (ARF network), whose address should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", then the device takes its address).
- LB0…LBF for one of the 16 loopback addresses or its name
- Any valid IPv4 or IPv6 address

Console path:

Setup > **NTP** > **RQ-Address**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.26.11.3 Authentication

Enables or disables MD5 authentication for the client.

Console path:

Setup > **NTP** > **RQ-Address**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

2.26.11.4 Key-ID

Identifies the key ID used for the client for MD5 authentication.

Console path:

Setup > **NTP** > **RQ-Address**

Possible values:

1 … 65535

2.26.12 RQ tries

Enter the number of times that synchronization with the time server should be attempted. Specifying a value of zero means that attempts will continue until a valid synchronization has been achieved.

Console path:

Setup > **NTP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.26.13 Authentication

Enables or disables MD5 authentication for the server.

Console path:

Setup > **NTP**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

2.26.14 Key

Configures the table **Authentication-Keys**.

Console path:

Setup > **NTP**

2.26.14.1 Key-ID

Identifies the key ID used for the server for MD5 authentication.

Console path:

Setup > **NTP** > **Authentication-Keys**

Possible values:

1 … 65535

2.26.14.2 Key

This entry contains the value of the key.

Console path:

Setup > **NTP** > **Authentication-Keys**

Possible values:

64 characters from `[A-Z@{|}~!$%&'()+-,/:;<=>?[\]^_.0-9a-z]`

2.26.15 Server-Trusted-Keys

Contains the list of trusted keys (comma-separated list of key numbers).

Console path:

Setup > **NTP**

Possible values:

Max. 63 characters from `[0-9,]`

2.26.16 Network list

This list contains the networks that your device uses as a time server.

Console path:

Setup > **NTP**

2.26.16.1 Network name

Defines the name of the network on which the NTP server is to be activated.

Console path:

Setup > **NTP** > **Networklist**

Possible values:

Entries from Setup/TCP-IP/Networklist: Characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.26.16.2 Server-Operating

Defines whether the NTP server is enabled on the selected network.

Console path:

Setup > **NTP** > **Networklist**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

2.26.17 Server-WAN-Access

Configures WAN access to your device.

Console path:

Setup > **NTP**

Possible values:

No

Disables access to the NTP server from the WAN.

Yes

Access from the WAN to the NTP server is possible via unmasked connections, but is in principle not possible with masked connections.

VPN

VPN access to the NTP server is enabled.

2.27 Mail

This menu contains the e-mail settings.

Console path:

Setup

2.27.1 SMTP server

Enter the name or the IP address for an SMTP server that you have access to. This information is required if your device is to inform you about certain events by e-mail.

A connection may be established in order to send e-mail messages. Please be aware that this may give rise to additional costs.

Console path:

Setup > **Mail**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.27.2 SMTP port

Enter the number of the SMTP port of the aforementioned server for unencrypted e-mail transmission. The default value is 587.

Console path:

Setup > **Mail**

Possible values:

Max. 10 characters from `[0-9]`

Default:

587

2.27.3 POP3 server

The only difference between names of many POP3 servers and SMTP servers is the prefix. All you have to do is enter the same of your SMTP server and replace "SMTP" with "POP" or "POP3".

Console path:

Setup > **Mail**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.27.4 POP3 port

Enter the number of the POP3 port of the aforementioned server for unencrypted mail. The default value is 110.

Console path:

Setup > **Mail**

Possible values:

Max. 10 characters from `[0-9]`

Default:

110

2.27.5 User name

Enter the name of the user who is to receive e-mail notifications at the aforementioned SMTP server.

Console path:

Setup > **Mail**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.27.6 Password

Enter the password to be used to send e-mail notifications to the aforementioned SMTP server.

Console path:

Setup > **Mail**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.27.7 E-mail sender

Enter here a valid e-mail address that your device is to use as a sender address for e-mailing notifications. This address is used by the SMTP servers to provide information in case of delivery problems. In addition, some servers check the validity of the sender e-mail address and deny delivery service if the address is missing, if the domain is unknown, or if the e-mail address is invalid.

Console path:

Setup > **Mail**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.27.8 Send again (min)

In case of connection problems with the SMTP server, mails will be buffered here and repeated tries will be made to send them. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the time after which an attempt will be made to re-submit buffered messages. Attempts are also made to re-submit each time a new e-mail is received.

Console path:

Setup > **Mail**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

2.27.9 Hold time (hrs.)

In case of connection problems with the SMTP server, mails will be buffered here and repeated tries will be made to send them. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the maximum hold time for a message. Once this time has elapsed, all attempts to submit a certain message will be discontinued.

Console path:

Setup > **Mail**

Possible values:

Max. 10 characters from `[0-9]`

Default:

72

2.27.10 Buffers

In case of connection problems with the SMTP server, mails will be buffered here and repeated tries will be made to send them. This also applies for mails which cannot be delivered due to incorrect settings such as incorrect SMTP parameters or unknown recipients. Set the maximum number of buffered messages. When this limit is exceeded, the oldest messages will be discarded to make room for incoming messages.

Console path:

Setup > **Mail**

Possible values:

Max. 10 characters from `[0-9]`

Default:

100

2.27.11 Loopback-Addr.

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address. If you have configured loopback addresses, you can specify them here as sender address.

If there is an interface called "DMZ", its name will be taken in this case.

Console path:

Setup > **Mail**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LB0 to LBF for the 16 loopback addresses.
Any valid IP address.

2.27.12 SMTP-use-TLS

Here you determine if and how the device encrypts the connection.

Console path:

Setup > **Mail**

Possible values:

No

No encryption. The device ignores any STARTTLS responses from the server.

Yes

The device uses SMTPS, and is therefore encrypted right from connection establishment.

Preferred

Connection establishment is not encrypted. If the SMTP server offers STARTTLS, the device starts encrypting.

Required

Connection establishment is not encrypted. If the SMTP server does not offer STARTTLS, the device does not transmits any data.

Default:

Preferred

2.27.13 SMTP-Authentication

Here you specify if and how the device authenticates at the SMTP server. The device's behavior depends on the server settings: If the server does not require authentication, the login occurs in any case. Otherwise, the device reacts according to the settings described below:

Console path:

Setup > **Mail**

Possible values:

None

Basically no authentication.

Plain text preferred:

The authentication preferably occurs in cleartext (PLAIN, LOGIN), if the server requires authentication. If it does not accept cleartext authentication, the device uses secure authentication.

Encrypted

The authentication is done without transmitting the password as cleartext (e.g., CRAM-MD5), if the server requires authentication. Cleartext authentication does not take place.

Preferred-Encrypted

The authentication is preferably encrypted (e.g., CRAM-MD5), if the server requires authentication. If it does not accept secure authentication, the device uses cleartext authentication.

Default:

Preferred-Encrypted

2.27.14 SSL

This sets the parameters for the SSL/TLS encryption used by the internal SMTP server.

Console path:

Setup > **Mail**

2.27.14.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Mail** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.27.14.2 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

Console path:

Setup > **Mail** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.27.14.3 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Mail** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly130

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly130

2.27.14.4 Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

Console path:

Setup > **Mail** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

SHA1

SHA2-256

SHA2-384

2.27.14.5 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **Mail** > **SSL**

Possible values:

No
Yes

Default:

Yes

2.27.14.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Mail** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.27.14.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Mail** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

ecdh_x25519
ecdh_x25519 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

ecdh_x25519

2.27.14.21 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Mail** > **SSL**

Possible values:

SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
SHA1-ECDSA
SHA224-ECDSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

2.30 IEEE802.1x

This menu contains the settings for the IEEE802.1x protocol.

Console path:

Setup

2.30.3 RADIUS server

To authenticate network clients a RADIUS server can be entered. Furthermore, a backup server can be specified for every RADIUS server.

Console path:

Setup > **IEEE802.1x**

2.30.3.1 Name

The name of the server.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.30.3.3 Port

The port the RADIUS server.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.30.3.4 Key

The secret used by the RADIUS server.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.30.3.5 Backup

You can enter the name of a backup server for the specified RADIUS server. The backup server will be connected only if the specified RADIUS server is unavailable. The name of the backup server can be selected from the same table.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.30.3.6 Loopback-Addr.

Here you can optionally configure a sender address to be used instead of the one used automatically for this destination address. If you have configured loopback addresses, you can specify them here as sender address.

If there is an interface called "DMZ", its address will be taken in this case.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LBO…LBF for the 16 loopback addresses.
Any IP address in the form `x.x.x.x`.

2.30.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

RADSEC
RADIUS

Default:

RADIUS

2.30.3.8 Host name

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server.

The RADIUS client automatically detects which address type is involved.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

2.30.3.9 Attribute-Values

With this entry you configure the RADIUS attributes of the RADIUS server.

The attributes are specified in a semicolon-separated list of attribute numbers or names (according to *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the form `<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2>`.

Variables can also be used as values (such as `%n` for the device name). Example: `NAS-Identifier=%n`.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.30.3.10 Sup.-Profile

Here you configure the menu Sup.-Profile.

Console path:

Setup > **IEEE802.1x** > **RADIUS-Server**

2.30.4 Ports

You should specify the login settings separately for each local network.

Console path:

Setup > **IEEE802.1x**

2.30.4 Port

The interface that this entry refers to.

Console path:

Setup > **IEEE802.1x** > **Ports**

2.30.4.4 Re-Auth-Max

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.30.4.5 Max-Req

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.30.4.6 Tx-Period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

2.30.4.7 Supp-Timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

2.30.4.7 Server timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

2.30.4.9 Quiet period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

Changes to these parameters require expert knowledge of the IEEE 802.1x standard. **Only make changes here if your system configuration absolutely requires them.**

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

60

2.30.4.10 Re-authentication

Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation. A typical value as a re-authentication interval is 3,600 seconds.

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

No
Yes

Default:

No

2.30.4.11 Re-Auth-Interval

A typical value as a re-authentication interval is 3,600 seconds.

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3600

2.30.4.12 Key transmission

Here you activate the regular generation and transmission of a dynamic WEP key.

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

No
Yes

Default:

No

2.30.4.13 Key-Tx-Interval

A typical value as a key-transmission interval is 900 seconds.

Console path:

Setup > **IEEE802.1x** > **Ports**

Possible values:

Max. 10 characters from `[0-9]`

Default:

900

2.30.4.14 Re-Auth-Delay-Period

Here you configure the wait time for re-authorization.

Console path:

Setup > **IEEE802.1x** > **Ports**

2.30.11 Supplicant-Setup

The keys used for encryption are automatically exchanged between the supplicant (client) and the AP on a regular basis.

The AP requires the supplicant to authenticate at regular intervals. As soon as the supplicant has successfully authenticated, it receives a new key from the AP which, from then on, is used for data transmission with the AP until a new key is exchanged.

Use this menu to configure the TLS settings for the supplicant.

Console path:

Setup > **IEEE802.1x**

2.30.11.13 TLS

This menu contains the TLS settings for the supplicant configuration.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup**

2.30.11.13.2 Versions

Specify the TLS version(s) that the supplicant uses for encryption.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

TLSv1
TLSv1.1
TLSv1.2

Default:

TLSv1

2.30.11.13.3 Key-exchange algorithms

Here you specify which algorithms are used for the key exchange between supplicant and AP.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.30.11.13.4 Crypto-Algorithms

Here you specify which crypto algorithms are used between supplicant and AP.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.30.11.13.5 Hash algorithms

Here you specify which hash algorithms are used between supplicant and AP.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.30.11.13.6 Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

Yes

Connections via PFS are preferred.

To turn this feature off, clear the check box.

Default:

Yes

2.30.11.13.8 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.30.11.13.22 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **IEEE802.1x** > **Supplicant-Setup** > **TLS**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.31 PPPoE-Server

This menu contains the settings for the PPPoE server.

Console path:

Setup

2.31.1 Operating

This switch enables and disables the PPPoE server.

Console path:

Setup > **PPPoE-Server**

Possible values:

No
Yes

Default:

No

2.31.2 Name list

In the list of peers/ remote sites, define those clients that are permitted access by the PPPoE server and define further properties and rights in the PPP list or the firewall.

Console path:

Setup > **PPPoE-Server**

2.31.2.1 Peer

Here you can set a peer name from the list of specified peers for each client. The peer name is to be used by the client as the PPP user name.

Console path:

Setup > **PPPoE-Server** > **Name-List**

2.31.2.2 SH time

Define the short-hold time for the PPPoE connection here.

Console path:

Setup > **PPPoE-Server** > **Name-List**

Possible values:

Max. 10 characters from `[0-9]`

Default:

empty

2.31.2.3 MAC address

If a MAC address is entered, then the PPP negotiation is terminated if the client logs on from a different MAC address.

Console path:

Setup > **PPPoE-Server** > **Name-List**

Possible values:

Max. 12 characters from `[0-9]`

Default:

000000000000

2.31.3 Service

The name of the service offered is entered under **Service**. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.

Console path:

Setup > **PPPoE-Server**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.31.4 Session limit

The "Session limit" specifies how often a client can be logged on simultaneously with the same MAC address. Once the limit has been reached, the server no longer responds to the client queries that are received. Default value is "1", maximum value "99". A Session limit of "0" stands for an unlimited number of sessions.

Console path:

Setup > **PPPoE-Server**

Possible values:

0 … 99

Default:

1

Special values:

0

switches the session limit off.

2.31.5 Ports

Here you can specify for individual ports whether the PPPoE server is active.

Console path:

Setup > **PPPoE-Server**

2.31.5.2 Port

From the list of ports available on the device, select the port which is to be activated or deactivated for the PPPoE server.

Console path:

Setup > **PPPoE-Server** > **Ports**

2.31.5.3 Enable PPPoE

Activates or deactivates the PPPoE server for the selected port.

Console path:

Setup > **PPPoE-Server** > **Ports**

Possible values:

No
Yes

Default:

Yes

2.31.6 AC-Name

This input field provides the option to give the PPPoE server a name that is independent of the device name (AC-Name = access concentrator name).

Console path:

Setup > **PPPoE-Server**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Special values:

empty

If you leave this field blank, the PPPoE server uses the device name as the server name.

Default:

empty

2.31.7 MTU-1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

Console path:

Setup > **PPPoE-Server**

Possible values:

Yes
No

Default:

No

2.32 VLAN

There are two important tasks when configuring the VLAN capabilities of the devices:

- Defining virtual LANs and giving each one a name, a VLAN ID, and allocating the interfaces
- For each interface, define how data packets with or without VLAN tags are to be handled

Console path:

Setup

2.32.1 Networks

The network list contains the name of each VLAN, the VLAN ID and the ports. Simply click on an entry to edit it.

Console path:

Setup > **VLAN**

2.32.1.1 Name

The name of the VLAN only serves as a description for the configuration. This name is not used anywhere else.

Console path:

Setup > **VLAN** > **Networks**

2.32.1.2 VLAN-ID

This number uniquely identifies the VLAN.

Console path:

Setup > **VLAN** > **Networks**

Possible values:

0 … 4096

Default:

0

2.32.1.4 Ports

Enter here the device interfaces that belong to the VLAN. For a device with a LAN interface and a WLAN port, ports that to be entered could include "LAN-1" and "WLAN-1". Port ranges are defined by entering a tilde between the individual ports: "P2P-1~P2P-4".

The first SSID of the first wireless LAN module is WLAN-1, and further SSIDs are WLAN-1-2 to WLAN-1-8. If the device has two WLAN modules, the SSIDs are called WLAN-2 and WLAN-2-2 to WLAN-2-8.

Console path:

Setup > **VLAN** > **Networks**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.32.1.5 LLDP-Tx-TLV-PPID

With this setting you use a comma-delimited list of interface names (analogous to the name in the **Ports** column) to decide which ports belonging to this VLAN are used by the device to propagate its membership via LLDP.

Console path:

Setup > **VLAN** > **Networks**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.32.1.6 LLDP-Tx-TLV-Name

With this setting you use a comma-delimited list of interface names (analogous to the name in the **Ports** column) to decide which ports belonging to this VLAN are used by the device to propagate the name of the VLAN via LLDP.

Console path:

Setup > **VLAN** > **Networks**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.32.2 Port table

The port table is used to configure each of the device's ports that are used in the VLAN. The table has an entry for each of the device's ports.

Console path:

Setup > **VLAN**

2.32.2.1 Port

The name of the port; this cannot be edited.

Console path:

Setup > **VLAN** > **Port-Table**

2.32.2.4 Allow all VLANs

This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.

Console path:

Setup > **VLAN** > **Port-Table**

Possible values:

No
Yes

Default:

Yes

2.32.2.5 Port-VLAN-Id

This port ID has two functions:

- Untagged packets received at this port in “Hybrid” mode are assigned to this VLAN, as are all ingress packets received in “Access” mode.
- In the “Hybrid” mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port receive no VLAN tag; all others are given a VLAN tag.

Console path:

Setup > **VLAN** > **Port-Table**

Possible values:

Max. 4 characters from `[0-9]`

Default:

1

2.32.2.6 Tagging-Mode

Controls the processing and assignment of VLAN tags at this port.

Console path:

Setup > **VLAN** > **Port-Table**

Possible values:

Access

Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.

Trunk

Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they will be dropped.

Hybrid

Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.

Default:

Hybrid

Tx-LLDP-TLV-Port-VLAN

Enables or disables the port as the LLDP-TLV port in this VLAN.

WEBconfig path: LCOS menu tree/Setup/VLAN/Port-Table/Tx-LLDP-TLV-Port-VLAN

Possible values:

- Yes
- No

Default: Yes

2.32.4 Operating

You should only activate the VLAN module if you are familiar with the effects this can have.

Faulty VLAN settings may cause access to the device's configuration to be blocked.

Console path:

Setup > **VLAN**

Possible values:

No
Yes

Default:

No

2.32.5 Tag value

When transmitting VLAN tagged networks via provider networks that use VLAN themselves, providers sometimes use special VLAN tagging IDs. In order for VLAN transmission to allow for this, the Ethernet2 type of the VLAN tag can be set as a 16-bit hexadecimal value as "tag value". The default is "8100" (802.1p/q VLAN tagging) other typical values for VLAN tagging could be "9100" or "9901".

Console path:

Setup > **VLAN**

Possible values:

Max. 4 characters from `[0-9][a-f]`

Default:

8100

2.32.6 S-Tag-Value

Defines the VLAN tagging ID for Q-in-Q VLAN tagging. The Ethernet2 type of the VLAN tag is a “tag value” configured as a 16-bit hexadecimal value. The default according to IEEE 802.1ad is “88a8”, and another common value for VLAN tagging would be “8100”, for example.

Console path:

Setup > **VLAN**

Possible values:

Max. 4 characters from `[0-9][a-f]`

Default:

88a8

2.33 Voice-Call-Manager

This menu contains the settings for the Call Manager.

Console path:

Setup

2.33.1 Operating

Switches the Call Manager on / off

Console path:

Setup > **Voice-Call-Manager**

Possible values:

No
Yes

Default:

No

2.33.2 General

This menu contains general settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

Possible values:

No
Yes

Default:

No

2.33.2.1 Domain

Name of the domain in which the connected telephones and the VoIP router are operated.

Terminal devices working in the same domain register as local subscribers at the VoIP router and make use of the SIP proxy.

Terminal devices working with the other domain of an active SIP PBX line register themselves as subscribers at an upstream PBX.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

Internal

2.33.2.2 Overlap timeout

When dialing from an ISDN telephone, this time period is waited until the called number is considered to be complete and then sent to the call router.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 99

Default:

6

Special values:

0

With a dial delay of "0", a "#" has to be entered at the end of the called number. Entering the "#" character after the called number manually reduces the dial delay.

2.33.2.3 Local-authentication

The SIP proxy usually accepts a registration from all SIP users who register themselves with a valid domain. If local authentication is forced, only those subscribers who are saved in one of the user tables with relevant access information can register with the SIP proxy.

Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users from the WAN and ISDN users must always be authenticated by a user entry with password.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

No
Yes

Default:

Yes

2.33.2.4 Echo canceler

Activates the echo canceling of remote echoes. With an echo that is too strong, subscribers can hear their own voices after a short delay. Activating this option reduces the echo at the SIP gateway.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

No
Yes

Default:

Yes

2.33.2.5 Outgoing packet reduction

For all SIP calls, sufficient bandwidth through the firewall is reserved as required by the audio codec being used (provided sufficient bandwidth is available). Here you can set how remaining data packets should be handled that are not part of SIP data streams in order to manage the firewall.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

PMTU reduction

The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU)

Fragmentation

The VoIP router reduces the data packets by fragmenting them to the required length.

None

The length of the data packets is not changed by the VoIP operation.

PMTU + Fragmentation

Default:

None

2.33.2.6 Incoming packet reduction

Similar to the outgoing data packets, you configure how non-VoIP data packets are handled when bandwidth is reserved for SIP data.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

PMTU reduction

The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU)

No change

The length of the data packets is not changed by the VoIP operation.

Default:

No change

2.33.2.7 Reduced packet size

This parameter specifies the packet size that should be used for PMTU adjustment or fragmentation while the SIP data have priority.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 9999

Default:

576

2.33.2.9 Country

The country setting determines the inband tones generated in the device

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Unknown
Austria
Belgium
Switzerland
Germany
France
Italy
Netherlands
Spain
Great Britain

Default:

Unknown

2.33.2.11 ClnPartyNumType

This sets the type of the calling number (CallingPartyNumber) for outgoing numbers on an ISDN interface. This is necessary for PBXs and exchanges in some countries as these require a specific type.

Functionality: "Auto" simply counts the number of leading zeros. If there are two or more, it is an international Number. If it is exactly a zero, then the number is a national number. In all other cases, the number is used as a subscriber number ("Subscriber"). The settings "Subscriber" and "National" also count the zeros, only set the type accordingly if the number (no zero or exactly one zero) is correct. Otherwise, the type is set to "Unknown".

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Subscriber
Unknown
National
auto

Default:

Subscriber

2.33.2.12 Register time

This value specifies the re-registration time that is signaled to a SIP user locally

This function allows the VoIP client to be registered at shorter intervals, so as to detect more quickly when a VoIP client has been switched off, for example.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

60 … 3600

Default:

120

2.33.2.13 Convert canonicals

This item activates the conversion of canonical VoIP names.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

No
Yes

Default:

Yes

2.33.2.15 SIP-DSCP

This defines which DiffServ CodePoints (DSCP) the SIP packets (for call signaling) are to be marked with.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

BE, CS-0, CS-1 … CS-7, AF-11 … AF-13, AF-21 … AF-23, AF-31 … AF-33, AF-41 … AF-43, EF
BE/CS-0, CS-1 … CS-7, AF-11 … AF-13, AF-21 … AF-23, AF-31 … AF-33, AF-41 … AF-43, EF
CS-6

Default:

CS-6

2.33.2.16 RTP-DSCP

This defines which DiffServ CodePoints (DSCP) the RTP packets (voice data stream) are to be marked with.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

BE, CS-0, CS-1 … CS-7, AF-11 … AF-13, AF-21 … AF-23, AF-31 … AF-33, AF-41 … AF-43, EF
BE/CS-0, CS-1 … CS-7, AF-11 … AF-13, AF-21 … AF-23, AF-31 … AF-33, AF-41 … AF-43, EF
EF

With DSCP set to BE or CS-0 the packets are sent unmarked. Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Default:

EF

2.33.2.17 Lock minutes

Specifies for how many minutes a SIP user will be blocked after authentication has failed due to incorrect login data.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 255 Minutes

Default:

5

Special values:

0

Lock off

2.33.2.18 Login errors

This value specifies the number of times a login fails before a SIP user account is locked for a set period.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 255

Default:

5

Special values:

0

The first false login triggers the lock.

2.33.2.19 T.38

This entry specifies whether T.38 in the Voice Call Manager is enabled or disabled.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

No
T.38 is disabled.

Yes
T.38 is enabled.

ISDN+Analog
T.38 is only active for ISDN and analog calls, not for SIP calls.

Default:

ISDN+Analog

2.33.2.20 VCM-DNS-Resolve

This switch allows SIP users to use the provider's domain to register with the device, provided that the device has a SIP line registered with this domain. The SIP client's DNS request for this provider domain is answered by the device with the local IP address. All SIP messages from this SIP client thus go directly to the device and are processed by its VCM (REGISTER initiates the registration of the client and an INVITE is forwarded via the SIP line specified in the call-routing table).

This switch is intended to make it easier to transition from using SIP clients without VCM to using VCM. In this case, all there is to do is configure the LANCOM device. There were occasional complications due to the automatic translation of the provider domain to the device IP, so this behavior can be changed here.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Yes
Automatic registration of SIP users is enabled.

No
Automatic registration of SIP users is disabled.

Default:

No

2.33.2.21 RTP-Port-Start

Use this field to set the first available RTP port in the RTP port range.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 65535

Default:

0

Special values:

0

Dynamic selection as long as RTP-Port-End is also set to "0".

2.33.2.22 RTP-Port-End

Use this field to set the last available RTP port in the RTP port range.

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

0 … 65535

Default:

0

Special values:

0

Dynamic selection as long as RTP-Port-Start is also set to "0".

2.33.2.23 Jitter buffer

With Voice over IP (VoIP), the transmission of data packets can be subject to jitter. This can diminish voice quality, and a jitter buffer is used to avoid this. This buffer compensates for a faulty or non-uniform data flow by temporarily buffering the incoming traffic.

Use this menu to configure the jitter buffer.

Console path:

Setup > **Voice-Call-Manager** > **General**

2.33.2.23.1 Mean-Jitter-Buffer-Factor

This entry specifies the average size of the jitter buffer in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 3 characters from `[0-9]`

Default:

16

2.33.2.23.2 Min-Jitter-Buffer

This entry specifies the minimum size of the jitter buffer in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 2 characters from `[0-9]`

Default:

2

2.33.2.23.3 Max-Jitter-Buffer

This entry specifies the maximum size of the jitter buffer in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 2 characters from `[0-9]`

Default:

2

2.33.2.23.4 Needed-Level-Time

Average value of the maximum delay time in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 2 characters from `[0-9]`

Default:

5000

2.33.2.23.5 Level-over-needed-Level

Maximum buffer size over needed buffer size in percent.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 2 characters from `[0-9]`

Default:

25

2.33.2.23.6 Target-Variance-Time

Desired variance time in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 5 characters from `[0-9]`

Default:

10000

2.33.2.23.7 AlgOn

Enables or disables the application layer gateway.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 1 characters from `[0-9]`

Default:

1

2.33.2.23.8 Long-Term-Deviation

This entry specifies the long-term deviation.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 2 characters from `[0-9]`

Default:

2

2.33.2.23.9 LTD-Time

This value specifies the time limit in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **General** > **Jitter-Buffer**

Possible values:

Max. 6 characters from `[0-9]`

Default:

5000

2.33.3 Users

This menu contains the user settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

2.33.3.1 SIP user

This menu contains the SIP user settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Users**

2.33.3.1.1 Users

This table is used to configure the users who are connected to the LAN via SIP. For the configuration of the user, it is unimportant if the LAN is accessed locally or via VPN (via the Internet). Along with SIP phones, you have also the option of setting up a SIP PBX as a user (internal SIP trunk connection).

The number of SIP users that can be created depends on the model. Entries with identical names or telephone numbers are not allowed.

The domain that is used by the SIP subscriber is usually configured in the terminal equipment itself.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

2.33.3.1.1.1 Number/Name

With this entry, you configure the phone number or the name of the SIP connection.

- Telephone number of the SIP phone
- Name of the user (SIP URI)
- Switchboard number of the SIP PBX, followed by a `#`. Your SIP PBX must be in the same network as your device, either locally or connected via VPN (internal SIP trunk connection).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.1.1.2 Auth-name

Name for authentication at the SIP proxy, and also to any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. This name is required if registration is mandatory (e.g. when logging in to an upstream SIP PBX or when "Force local authentication" is set for local users).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Special values:

empty

If nothing is entered here, the authentication is attempted using the SIP name (internal call number).

2.33.3.1.1.3 Secret

Password for authentication to the SIP proxy, and also to any upstream SIP PBX, when the user's domain is the same as the domain of a SIP PBX line. It is possible for users to log in to the local SIP proxy without authentication ("Force local authentication" is deactivated for SIP users) and where applicable to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.1.1.4 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

No
Yes

Default:

Yes

2.33.3.1.1.5 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.1.1.6 Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Phone
Fax
Auto

Default:

Phone

2.33.3.1.1.7 CLIR

Switches the transmission of the calling-line identifier on/off.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

No

Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Yes

Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.

Default:

No

2.33.3.1.1.8 Access from WAN

This item determines whether and how SIP clients can register via a WAN connection.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

No
VPN

Default:

No

2.33.3.1.1.20 DTMF-Method

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Inband

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

SIP-INFO

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

RTP-Event

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

RTP-Event/SIP-Info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

Default:

RTP-Event

2.33.3.1.1.21 MWI target line

Voice and messages left on your provider mailbox are signaled by notifications on the device. For the configured SIP users, select the line that is to be enabled for this function.

Notification only occurs if the provider supports this function.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User** > **Users**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]"{|}%<>[]`

Default:

empty

2.33.3.1.1.22 Transport

This entry is used to select a protocol used by this user to communicate with the local SIP server.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

UDP

All SIP packets to this SIP user are transmitted via connectionless UDP. Most SIP users support this setting.

TCP

All SIP packets to this SIP user are transmitted via connection-oriented TCP. For this purpose, a TCP connection is established and maintained for the duration of the registration.

TLS

Like TCP, but all of the SIP packets are encrypted.

Default:

UDP

TCP

TLS

2.33.3.1.1.23 SRTP

With this entry, you configure the secure real-time transport protocol (SRTP) for the encryption and transmission of SIP-user authentication data.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

Reject

Encryption is not proposed for this user's calls. Calls by this user with an encryption proposal are rejected. The voice channel is never encrypted.

Ignore

Encryption is not proposed for calls by this user. Calls by this user with an encryption proposal are also accepted. However, the voice channel is never encrypted.

Prefer

Encryption is offered for this user's calls. Calls by this user without an encryption proposal are accepted. The voice channel is only encrypted if the user supports encryption.

Forced

Encryption is offered for this user's calls. Calls by this user without an encryption proposal will fail. The speech channel is either encrypted or is not established.

Default:

Ignore

2.33.3.1.1.24 SRTP ciphers

Here you select the encryption method for communications with the user.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

AES-CM-256
Encryption uses the AES256 method and a key length of 256 bits.

AES-CM-192
Encryption uses the AES192 method and a key length of 192 bits.

AES-CM-128
Encryption uses the AES128 method and a key length of 128 bits.

F8-128
Encryption uses the F8-128 method and a key length of 128 bits.

Default:

AES-CM-256

AES-CM-192

AES-CM-128

F8-128

2.33.3.1.1.25 SRTP-Message-Auth-Tags

Here you specify the authentication method for this user.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

HMAC-SHA1-80
Authentication is performed using the hash algorithm HMAC-SHA1-80 (hash length 80 bits).

HMAC-SHA1-32
Authentication is performed using the hash algorithm HMAC-SHA1-32 (hash length 32 bits).

Default:

HMAC-SHA1-80

HMAC-SHA1-32

2.33.3.1.2 Intern-Cln-Prefix

If an incoming internal call is directed to a SIP user, this prefix is added to the calling party ID, if available.

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a "0". All other calls are regarded as internal.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

*

2.33.3.1.3 Extern-Cln-Prefix

If an incoming external call is directed to a SIP user, this prefix is added to the calling party ID, if available.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **SIP-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

empty

2.33.3.2 ISDN user

This menu contains the ISDN user settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Users**

2.33.3.2.1 Interfaces

Here you select the interface that the ISDN user is connected to.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User**

2.33.3.2.1.1 Name

Name of interface

Console path:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

Possible values:

ISDN

Default:

ISDN

2.33.3.2.1.2 Ifc

From the available ISDN interfaces, select the ISDN interface that the ISDN subscribers are connected to, e.g. S0-1 or S0-2.

The choices are different depending on the model.

Console path:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

Possible values:

ISDN

Default:

ISDN

2.33.3.2.1.3 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

Possible values:

No
Yes

Default:

Yes

2.33.3.2.1.4 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.2.1.5 Local code

Specify the area code for the interface of the ISDN user.

Console path:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

2.33.3.2.2 Users

Here you can define all local ISDN users (terminal devices). You can also specify the authentication data for SIP registration.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User**

2.33.3.2.2.1 Number/Name

Internal number of the ISDN telephone or name of the user (SIP URI).

By using the # character as a placeholder, entire groups of numbers (e.g. when using extension numbers at a point-to-point connection) can be addressed via a single entry. With the number "#" and the DDI "#", for example, extension numbers can be converted into internal telephone numbers without making any changes. With the call number "3#" and the DDI "#", for example, an incoming call for extension "55" is forwarded to the internal number "355", and for outgoing calls from the internal number "377", the extension number "77" will be used.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

2.33.3.2.2.2 Ifc

ISDN interface that should be used to establish the connection.

The choices and the default setting depend on the device type.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

2.33.3.2.2.3 MSN/DDI

Internal MSN that is used for this user on the internal ISDN bus.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

MSN

Number of the telephone connection if it is a point-to-multipoint connection.

DDI (Direct Dialing in)

Telephone extension number if the connection is configured as a point-to-point line.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 19 characters from `[0-9]#`

Default:

empty

2.33.3.2.2.4 Display name

Name for display on the telephone being called.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default:

empty

2.33.3.2.2.5 Auth-name

Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

Only required when the user registers at an upstream SIP PBX.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.3.2.2.6 Secret

Password for authentication as a SIP user at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.3.2.2.7 Domain

Domain of an upstream SIP PBX when the ISDN user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

Only required when the user registers at an upstream SIP PBX.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.3.2.2.8 DialCompl

En-block dial detection allows the dialed number to be marked as complete (e.g. for speed dialing or repeat dialing) so that the call is established more quickly. Suffix dialing is not possible.

The number can be manually marked as complete with "#" and the call can be initiated.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Auto

Block dialing is detected automatically (for example, with speed dial or repeat dialing), so that the call is established more quickly. Suffix dialing is not possible.

Manual:

No block dialing; the number can be marked as complete with "#" and the call can be initiated.

Default:

Auto

2.33.3.2.2.9 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

No
Yes

Default:

Yes

2.33.3.2.2.10 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.2.2.11 Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

Phone
Fax
Auto

Default:

Phone

2.33.3.2.2.12 CLIR

Switches the transmission of the calling-line identifier on/off.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

No

Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Yes

Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.

Default:

No

2.33.3.2.2.13 Parallel call

Enables or disables parallel calls.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User** > **Users**

Possible values:

No

Parallel call is disabled.

Yes

Parallel call is enabled.

Default:

No

2.33.3.2.3 Intern-Cln-Prefix

If an incoming internal call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

*

2.33.3.2.4 Extern-Cln-Prefix

If an incoming external call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

empty

2.33.3.2.5 Intern-Dial-Tone

The dial tone determines the sound a user hears after lifting the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone to the use for spontaneous outside-line access to simulate the behavior of an external connection.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **ISDN-User**

Possible values:

No

The external dial tone is used.

Yes

Default:

No

2.33.3.2.6 CldPartyNumType

This sets the type of the called number (CalledPartyNumber) for incoming numbers on an ISDN telephone.

Functionality: "Auto" simply counts the number of leading zeros. If there are two or more, it is an international Number. If it is exactly a zero, then the number is a national number. In all other cases, the number is used as a subscriber number ("Subscriber"). The settings "Subscriber" and "National" also count the zeros, only set the type accordingly if the number (no zero or exactly one zero) is correct. Otherwise, the type is set to "Unknown".

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Subscriber
Unknown
National
auto

Default:

Subscriber

2.33.3.2.7 ClnPartyNumType

This sets the type of the calling number (CallingPartyNumber) for outgoing numbers on an ISDN telephone.

Functionality: "Auto" simply counts the number of leading zeros. If there are two or more, it is an international Number. If it is exactly a zero, then the number is a national number. In all other cases, the number is used as a subscriber number ("Subscriber"). The settings "Subscriber" and "National" also count the zeros, only set the type accordingly if the number (no zero or exactly one zero) is correct. Otherwise, the type is set to "Unknown".

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

Subscriber
Unknown
National
auto

Default:

Unknown

2.33.3.3 Analog user

This menu contains the settings for analog users.

Console path:

Setup > **Voice-Call-Manager** > **Users**

2.33.3.3.1 Interfaces

This table contains the configuration settings for the analog interfaces.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User**

2.33.3.3.1.1 Name

This entry contains the name of the interface (e.g. "ANALOG").

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Interfaces**

2.33.3.3.1.2 Ifc

This entry displays the available interfaces for which the configuration is to apply.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Interfaces**

Possible values:

Analog-1
Analog-2

Default:

Analog-1

Analog-2

2.33.3.3.1.3 Active

This entry enables or disables the selected interface.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Interfaces**

Possible values:

No
Yes

Default:

Yes

2.33.3.3.1.4 Comment

Enter a comment about this configuration.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Interfaces**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.3.2 Users

This menu contains the user settings.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User**

2.33.3.3.2.1 Number/Name

Enter a number or name for the user who these settings apply to.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.2 Ifc

Select the Analog interfaces which should be alerted when a call is made to the number entered in the field **Number/Name**.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Analog-1
Analog-2
Analog-3
Analog-4
none
all

Default:

all

2.33.3.3.2.3 Display name

Here you specify the name or the number used to display the user.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.4 Auth-name

Use this entry to set the name used by the user to authenticate at the Voice Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.5 Secret

Set the user password for verification at the Voice Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.6 Domain

Enter a valid VoIP domain here.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.8 CLIR

This entry switches the transmission of the calling-line identifier on/off.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

No

Transmission of the calling-line identifier is not suppressed in the device; the settings in the user's terminal device control the transmission of the calling-line identifier.

Yes

Transmission of the calling-line identifier is suppressed whatever the setting in the user's device.

Default:

No

2.33.3.3.2.9 Metering

This entry enables or disables the charge metering.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

No

Call charges are not metered.

Yes

Call charges are metered.

Default:

No

2.33.3.3.2.10 Active

This entry enables the corresponding user for the Voice Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

No

User is disabled.

Yes

User is enabled.

Default:

Yes

2.33.3.3.2.11 Comment

Enter a comment about this user.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.3.2.12 Device type

Use this entry to specify the device type for which these settings apply.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User** > **Users**

Possible values:

Phone
Fax
Auto
Modem

Default:

Phone

2.33.3.3.2.13 DialIfc

Select an Analog interface. A telephone connected to this interface uses the number entered in the field **Number/Name** as a source number when it makes a call.

Pfad Konsole:

Setup > **Voice-Call-Manager** > **User** > **Analog-User** > **Users**

Mögliche Werte:

Analog-1
Analog-2
Analog-3
Analog-4
none
all

Default-Wert:

all

2.33.3.3.3 Intern-Cln-Prefix

If an incoming internal call is directed to an analog user, this prefix is added to the calling party ID, if available.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

empty

2.33.3.3.4 Extern-Cln-Prefix

If an incoming external call is directed to an analog user, this prefix is added to the calling party ID, if available.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User**

Possible values:

Max. 15 characters from `[0-9]*`

Default:

empty

2.33.3.3.5 Intern-Dial-Tone

The dial tone determines the sound a user hears after lifting the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone to the use for spontaneous outside-line access to simulate the behavior of an external connection.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Analog-User**

Possible values:

No

The external dial tone is used.

Yes

Default:

No

2.33.3.4 Extensions

Here you can define extended user settings such as call waiting or call forwarding.

Console path:

Setup > **Voice-Call-Manager** > **Users**

Possible values:

No

The external dial tone is used.

Yes

Default:

No

2.33.3.4.1 Name

The user settings apply to this telephone number or SIP-ID.

Call forwarding can be set up for all local users (SIP, ISDN or analog).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.4.2 User modifiable

This activates or deactivates the option for users to configure their settings via the telephone.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

Yes

2.33.3.4.3 CFU active

Activates or deactivates the immediate forwarding of calls (CFU).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

No

2.33.3.4.4 CFU active

Destination for immediate unconditional call forwarding.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.3.4.5 CFNR active

Activates or deactivates the delayed forwarding of call (after waiting for no reply).

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

No

2.33.3.4.6 CFNR target

Destination for call forwarding no reply.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.4.7 CFNR timeout

Wait time for call forwarding on no reply. After this time period the call is forwarded to the target number if the subscriber does not pick up the phone.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

0 … 255 Seconds

Default:

15

2.33.3.4.8 CFB active

Activates or deactivates call forwarding on "busy".

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

No

2.33.3.4.9 CFB target

Target for call forwarding on "busy".

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.3.4.10 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

Yes

2.33.3.4.11 Busy-on-Busy

Prevents a second call from being connected to a terminal device, irrespective of whether CW (call-waiting indication) is active on the device or not; i.e. there is no "call waiting" signal. The second caller hears an engaged tone. This also applies where an internal telephone number supports multiple logins and just one of the possible terminal devices is already in use.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

No
Yes

Default:

No

2.33.3.4.12 CF-Set-Cln-Id

Use this entry to set which phone number will be signaled when a call is forwarded (CF) - for example from CDIV - alternatively, you can enter your own phone number as a fixed setting.

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Extension-ID
Calling ID

Signals the incoming phone number. When the call is forwarded to a mobile phone, a subscriber will be able to identify the caller's original phone number.

Custom ID

Signals the phone number entered under **Setup** > **Voice-Call-Manager** > **Users** > **Extensions** > **Custom-ID**.

Default:

Extension-ID

2.33.3.4.13 Custom ID

Use this entry to set the phone number that will be used for signaling with call forwarding.

This phone number will only be used if the parameter **Setup** > **Voice-Call-Manager** > **Users** > **Extensions** > **CF-Set-Cln-Id** is set to "Custom-ID".

Console path:

Setup > **Voice-Call-Manager** > **Users** > **Extensions**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4 Lines

This menu contains the line settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

2.33.4.1 SIP provider

This menu contains the SIP provider settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Lines**

2.33.4.1.1 Lines

The device uses these lines to register with other SIP remote stations (usually SIP providers or remote gateways at SIP PBXs). The connection is made either over the Internet or a VPN tunnel. You can enter up to 16 SIP lines.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider**

2.33.4.1.1.1 Name

Name of the line; may not be identical to another line that is configured in the device.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.4.1.1.2 Domain

SIP domain/realm of the upstream device. Provided the remote device supports DNS service records for SIP, this setting is sufficient to determine the proxy, outbound proxy, port and registrar automatically. This is generally the case for typical SIP provider services.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.4.1.1.3 Port

TCP/UDP port that the SIP provider uses as the target port for SIP packets.

This port has to be activated in the firewall for the connection to work.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

0 … 65535

Default:

5060

2.33.4.1.1.4 User ID

Telephone number of the SIP account or name of the user (SIP URI).

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.1.1.5 Auth-name

Name for authentication to the upstream SIP device (provider/SIP PBX).

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.1.1.6 Secret

The password for authentication at the SIP registrar and SIP proxy at the provider. For lines without (re-)registration, the password may be omitted under certain circumstances.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.1.1.8 Cln-Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 9 characters from `[0-9]`

Default:

empty

2.33.4.1.1.9 Number/Name

The effect of this field depends upon the mode set for the line:

If the line is set to "Single account" mode, all incoming calls on this line with this number as the destination (SIP: "To:") are transferred to the call router.

If the mode is set to "Trunk", the destination number is determined by removing the trunk's switchboard number. If an error occurs, the call will be supplemented with the number entered in this field (SIP: "To:") are transferred to the call router.

If mode is set to "Gateway" or "Link" the value entered in this field has no effect.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.1.1.10 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Yes

Default:

Yes

2.33.4.1.1.11 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.1.1.14 Rtg tag

Routing tag for selecting a certain route in the routing table for connections to this SIP provider.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[0-9]`

Default:

0

2.33.4.1.1.15 Display name

Name for display on the telephone being called.

Normally this value should not be set as incoming calls have a display name set by the SIP provider, and outgoing calls are set with the local client or call source (which may be overwritten by the user settings for display name, if applicable). This settings is often used to transmit additional information (such as the original calling number when calls are forwarded) that may be useful for the person called. In the case of single-line SIP accounts, some providers require an entry that is identical to the display name defined in the registration details, or the SIP ID (e.g. T-Online). This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored there or on the terminal device, then the line type "SIP PBX line" should be selected.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[0-9]`

Default:

empty

2.33.4.1.1.16 Registrar

The SIP registrar is the point at the SIP provider that accepts the login with the authentication data for this account.

This field can remain empty unless the SIP provider specifies otherwise. The registrar is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 64 characters from `[0-9]`

Default:

empty

2.33.4.1.1.17 Mode

This selection specifies the operating mode of the SIP line.

The "Service provider" can be a server in the Internet, an IP PBX, or a voice gateway. Please observe the notices about "SIP mapping".

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Provider

Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal destination number. Only one connection can exist at a time.

Trunk

Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main switchboard number with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: “From:”). For incoming calls, the prefix is removed from the destination

number (SIP: "To:"). The remaining digits are used as the internal extension number. In case of error (prefix not found, destination equals prefix) the call is forwarded to the internal destination number as configured. The maximum number of connections at any one time is limited only by the available bandwidth.

Gateway

Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: "From:") and sent in a separate field (SIP: "Contact:"). For incoming calls the dialed number (destination) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Link

Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP: "From:") is not modified. For incoming calls, the dialed number (destination; SIP: "To:") is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Flex

- To the outside the line behaves like a commercially available SIP account with a single public number.
- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

Default:

Provider

2.33.4.1.1.18 Refer forwarding

Call switching (connect call) between two remote subscribers can be handled by the device itself (media proxy) or it can be passed on to the exchange at the provider if both subscribers can be reached on this SIP provider line (otherwise the media proxy in the device assumes responsibility for switching the media streams, for example when connecting between two SIP providers).

An overview of the main SIP providers supporting this function is available in the Support area of our homepage.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No

Switching is retained within the device.

Yes

Switching is passed on to the provider.

Default:

No

2.33.4.1.1.19 Local port

This is the port used by the proxy to communicate with the provider.

If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered at the provider end as the destination port (e.g. when using an unregistered trunk in the company VPN). This ensures that both ends can send SIP signaling.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

1 … 65536

Default:

0

Special values:

0

Dynamic port selection; the port is automatically selected from the pool of available port numbers.

2.33.4.1.1.20 (Re-) registration

This activates the (repeated) registration of the SIP provider line. Registration can also be used for line monitoring.

To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the provider's SIP registrar suggests a different interval, the suggested value is used automatically.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Yes

Default:

Yes

2.33.4.1.1.21 Line control method

Specifies the line monitoring method. Line monitoring checks if a SIP provider line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Auto

The method is set automatically.

Inactive

No monitoring; the line is always reported as being available. This setting does not allow the actual line availability to be monitored.

Register

Monitoring by means of register requests during the registration process. This setting also requires "(Re-)registration" to be activated for this line.

Options

Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e.g. lines without registration.

Default:

Auto

2.33.4.1.1.22 Line control interval

The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

Values less than 60 seconds are automatically set to 60 seconds.

If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

2.33.4.1.1.23 Trustworthy

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

The function is not supported by all providers.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Not trusted

Yes
Trusted

Default:

Yes

2.33.4.1.1.24 Privacy method

Specifies the method used for transmitting the caller ID in the separate SIP-header field.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

None

RFC3325
By P-Preferred-Id/P-Asserted-Id

IETF-Draft-Sip-Privacy-04
By RPID (Remote Party ID)

Default:

None

2.33.4.1.1.25 remove-FROM-usertype

Select this option to remove the "user=phone" information from the From field for outgoing calls over a provider line. Some VoIP proxies do not process this information according to the standard and reject the call.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Yes

Default:

No

2.33.4.1.1.26 Trunk-Inc-Cld-In-ToHeader

Using this setting you enable or disable the work-around for the case that the provider transmits the complete destination number (switchboard number + extension) not in the Request line but in the TO-URI, and the number in the "To" field is not necessarily longer than the number in the Request line. You should leave this setting enabled to ensure compatibility with these providers.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Yes

Default:

No

2.33.4.1.1.27 DTMF-Method

Depending on the requirements, it may not be sufficient to transmit “inband” DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Inband

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

SIP-INFO

The DTMF tones are transmitted “out-of-band” as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

RTP-Event

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

RTP-Event/SIP-Info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

Default:

RTP-Event

2.33.4.1.1.28 Transport

Use this entry to specify which protocol is used to encrypt the data streams.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Auto

NAPTR (Naming Address Pointer) records are used for DNS resolution. In the DNS data, the provider specifies the use of transport protocols such as UDP, TCP or TLS. The provider can also specify weights or priorities.

If TLS is specified as the transport protocol for signaling encryption by NAPTR, voice encryption is also used automatically, regardless of the explicit configuration setting of voice encryption.

UDP

All SIP packets are transmitted connectionless. Most providers support this setting.

TCP

All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.

TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider. The TLS version selected in the configuration is taken as the minimum requirement for TLS encryption.

Default:

Auto

2.33.4.1.1.29 SRTP

Use this entry to specify how SRTP (secure real-time transport protocol) is handled.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Reject
Ignore
Preferred
Forced

Default:

Ignore

2.33.4.1.1.30 Strict-Mode

This option activates a security mechanism that stops the SIP user agent from processing SIP messages from unknown VoIP servers, which could otherwise lead to SIP calls being diverted or disconnected, for example.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
The strict mode is disabled.

Yes
The strict mode is enabled.

Default:

Yes

2.33.1.1.32 Verify server certificate

With this setting you specify whether the certificate produced by the SIP server when establishing the TLS connection is to be classified as trustworthy and accepted.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No verification
The server certificate is not verified. All valid server certificates are accepted, whichever CA they were signed by. This setting is useful for accepting self-signed certificates.

Accept trusted

The server certificate is verified against all CAs known to the LANCOM. These include all CAs that LCOS "knows" to be trusted and also those from the VoIP server certificate slots 1 to 3.

The encrypted connection is only established if one of these certificates is validated successfully.

SIP-Trusted-CA-Slot-1

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 1 of the VoIP certificates.

SIP-Trusted-CA-Slot-2

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 2 of the VoIP certificates.

SIP-Trusted-CA-Slot-3

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 3 of the VoIP certificates.

Telekom-Shared-Business-CA4

With this setting, the device only accepts server certificates signed by the Telekom Shared Business CA4 CA.

Use this setting for SIP trunk connections from Deutsche Telekom AG.

Default:

No verification

2.33.4.1.1.33 Allow inbound UDP from

With this setting you specify the network context in which the device accepts a UDP packet.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

LAN
VPN
WAN

Default:

LAN

VPN

WAN

2.33.4.1.1.34 SRTP ciphers

This item allows you to select the encryption method for the SIP line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

AES-CM-256

Encryption uses the AES256 method and a key length of 256 bits.

AES-CM-192

Encryption uses the AES192 method and a key length of 192 bits.

AES-CM-128

Encryption uses the AES128 method and a key length of 128 bits.

F8-128

Encryption uses the F8-128 method and a key length of 128 bits.

2.33.4.1.1.35 SRTP-Message-Auth-Tags

Use this item to specify the authentication method for this SIP line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

HMAC-SHA1-80

Authentication is performed using the hash algorithm HMAC-SHA1-80 (hash length 80 bits).

HMAC-SHA1-32

Authentication is performed using the hash algorithm HMAC-SHA1-32 (hash length 32 bits).

2.33.4.1.1.36 Overlap dialing

This is where you enable or disable overlap dialing.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

0

Deactivated

1

Activated

Default:

0

2.33.4.1.1.37 Registration interval

Set the registration interval in seconds.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

1 … 3600

Default:

480

2.33.4.1.1.38 Fallback

Configures the fallback mechanism for the SIP provider line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No

No fallback to an unencrypted connection is performed. If it is not possible to establish an encrypted connection to the VoIP provider, the line remains unregistered.

UDP

As a rule, encrypted SIP connections are made with the TCP protocol and unencrypted connections are made with the UDP protocol. This setting switches directly to an unencrypted UDP connection if the encrypted TCP connection cannot be established.

Complete

If an encrypted TCP connection with the configured TLS version cannot be established, then attempts are made to establish an unencrypted TCP connection, and finally a UDP connection in order to register the VoIP line.

This setting provides the best compatibility, but may lead to a longer registration time.

Default:

No

2.33.4.1.1.39 User-Id-Field

Specifies the field used to transmit the SIP ID.

With a single account, outgoing calls always signal the SIP ID in the FROM field.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

PAI-PPI

The SIP ID including the DDI is transmitted via the PPI / PAI. The source telephone number is transmitted via the FROM field.

From

The SIP ID is transmitted via the FROM field. The source telephone number is transmitted via the PPI / PAI field.

None

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI / PAI.

PPI-woDDI

In contrast to the P-Preferred-Identity, an extension number (DDI) is not transmitted in the SIP ID via the PPI.

PPI-PPI

The SIP ID including the DDI is transmitted via the PPI. The source telephone number is transmitted via the FROM field.

None-PPI

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI.

None-PAI

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PAI.

Default:

PAI-PPI

2.33.4.1.1.41 Allow SIP302-forwarding

Activates call forwarding at the SIP provider by using SIP 302.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

No
Yes

Default:

No

2.33.4.1.1.42 Tcp-Timeout

Sets the TCP timeout to a fixed value (in seconds). If a SIP server is not reachable, Voice Call Manager aborts the connection attempt after the TCP timeout expires and establishes a connection to the next SIP server. This greatly reduces the waiting time when switching servers if the first contacted SIP server is not reachable.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

0 … 255 seconds

Default:

5

2.33.4.1.2 Mapping

The entries made under SIP mapping establish a series of rules for number translation to SIP lines in the trunk or gateway mode. Up to 40 mapping rules can be entered.

A SIP line in trunk mode is used for mediating between internal numbers and the range of telephone numbers offered by a SIP account.

For incoming calls, the destination number (called party ID) is modified. The internal number is used if the called party ID matches with the external telephone number.

For outgoing calls, the calling party ID is modified. The external number is used if the calling party ID matches with the internal telephone number.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider**

2.33.4.1.2.1 SIP provider

From the list of defined SIP lines, select the name of the line which the telephone number mapping applies to.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

2.33.4.1.2.2 Ext-Number/Name

Call number within the range of those used by the SIP trunk account or upstream SIP PBX.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.1.2.3 Number/Name

Telephone number in the range of the VoIP router.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.1.2.4 Length

The value defines the number of digits required for a called number to be considered as complete. It only applies to SIP gateway lines with entries that end in a # symbol.

For an outgoing call, the external called number generated from this entry is automatically regarded as complete according to the defined number of numerals, and then forwarded. This process speeds up the dialing process. Alternatively, the called number is regarded as complete when:

The user concludes the dialed number with a # symbol, or

a precisely matching entry was found in the SIP mapping table without a # symbol, or

the wait time expires.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

Max. 9 characters from `[0-9]`

Default:

0

Special values:

0

By setting the length of called number to "0" you deactivate the premature dialing of the called number based on its length.

2.33.4.1.2.5 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

No
Yes

Default:

Yes

2.33.4.1.2.6 Comment

Comment on this entry

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.4.1.2.7 CLIR

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Mapping**

Possible values:

No
Yes

Default:

No

2.33.4.1.3 Dynamic-Line

Configure the dynamic SIP lines here.

Console path:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider**

2.33.4.1.3.1 Dynamic-Line-Name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[]^_.`

2.33.4.1.3.2 SIP-Line-Name

Here you specify one of the already configured physical SIP connections.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[]^_.`

2.33.4.1.3.3 Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 3 characters from `[0-9]`

2.33.4.1.3.4 Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 3 characters from `[0-9]`

2.33.4.1.3.5 Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Weight

This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin

With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority

The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

2.33.4.1.3.6 Max-Calls

Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 3 characters from `[0-9]`

2.33.4.2 SIP-PBX

This menu contains the SIP PBX settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Lines**

2.33.4.2.1 SIP-PBX

You use these lines to configure connections to upstream SIP PBXs, which are usually connected via VPN. You can enter up to 4 SIP PBXs.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

2.33.4.2.1.1 Name

Name of the line; may not be identical to another line that is configured in the device.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.2.1.2 Domain

SIP domain/realm of the upstream SIP PBX.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.2.1.3 Port

TCP/UDP port of the upstream SIP PBX to which the device sends the SIP packets.

This port has to be activated in the firewall for the connection to work.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

0 … 65535

Default:

5060

2.33.4.2.1.4 Secret

Shared password for registering with the SIP PBX. This password is only required (a) when SIP subscribers have to log in to the PBX who have not been set up as SIP users with their own access data in the SIP user list or (b) when local SIP authentication is not forced. This means that SIP users can register with the device without a password and can log in to the upstream SIP PBX with a shared password if the SIP user's domain is the same as the domain of a SIP PBX line.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.2.1.6 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

No
Yes

Default:

Yes

2.33.4.2.1.7 Comment

Comment on this entry

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.2.1.8 Cln-Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

For example; a number can be added, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 9 characters from `[0-9]`

Default:

empty

2.33.4.2.1.9 Line prefix

With outgoing calls using this line, this prefix is placed in front of the calling number to create a complete telephone number that is valid for this line. With incoming calls this prefix is removed, if present.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 9 characters from `[0-9]`

Default:

empty

2.33.4.2.1.12 Rtg-Tag

Routing tag for selecting a certain route in the routing table for connections to this SIP PBX.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 64 characters from `[0-9]`

Default:

0

2.33.4.2.1.13 Registrar

The SIP registrar is the point that accepts the login with the configured authentication data for this account in the SIP PBX.

This field can remain empty unless the SIP provider specifies otherwise. The address of the registrar is resolved over the realm.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.2.1.14 Local port

This is the port used by the proxy to communicate with the upstream SIP PBX.

If line (re-)registration is deactivated, the local port has to be defined with a fixed value, and this also has to be entered into the SIP PBX to ensure that both ends can send SIP signaling.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

1 … 65536

Default:

0

Special values:

0

Dynamic port selection; the port is automatically selected from the pool of available port numbers.

2.33.4.2.1.15 (Re-) registration

This activates the (repeated) registration of the SIP PBX line. Registration can also be used for line monitoring.

To use (re-) registration, the line monitoring method must correspondingly be set to "Register" or "Automatic". Registration is repeated after the monitoring interval has expired. If the SIP registrar in the SIP PBX suggests a different interval, the suggested value is used automatically.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

No
Yes

Default:

Yes

2.33.4.2.1.16 Line monitoring

Specifies the line monitoring method. Line monitoring checks if a SIP PBX line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Auto

The method is set automatically.

Deactivated

No monitoring; the line is always reported as being available. This setting does not allow the actual line availability to be monitored.

Options

Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e.g. lines without registration.

Default:

Auto

2.33.4.2.1.17 Monitoring interval

The monitoring interval in seconds. This value affects the line monitoring with register request and also the option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again. If (re-) registration is activated, the monitoring interval is also used as the time interval before the next registration.

Values less than 60 seconds are automatically set to 60 seconds.

If the remote station responds to an option request with a different suggested value for the monitoring interval, this is accepted and subsequently applied.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

2.33.4.2.1.18 Trusted

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.

Please note that not all providers support this function.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

No
Not trusted

Yes
Trusted

Default:

Yes

2.33.4.2.1.19 Privacy method

Specifies the method used for transmitting the caller ID in the separate SIP-header field.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX**

Possible values:

None

RFC3325
By P-Preferred-Id/P-Asserted-Id

IETF-Draft-Sip-Privacy-04
By RPID (Remote Party ID)

Default:

None

2.33.4.2.1.20 DTMF-Method

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Console path:

Setup > **Voice-Call-Manager** > **Line** > **SIP-PBX** > **PBX**

Possible values:

Inband
The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

SIP-INFO
The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

RTP-Event
The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

RTP-Event/SIP-Info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

Default:

RTP-Event

2.33.4.2.1.21 Strict-Mode

This option activates a security mechanism that stops the SIP user agent from processing SIP messages from unknown VoIP servers, which could otherwise lead to SIP calls being diverted or disconnected, for example.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX** > **PBX**

Possible values:

No

The strict mode is disabled.

Yes

The strict mode is enabled.

Default:

Yes

2.33.4.2.1.22 Allow inbound UDP from

With this setting you specify the network context in which a UDP packet is accepted.

Console path:

Setup > **Voice-Call-Manager** > **Line** > **SIP-PBX** > **PBX**

Possible values:

LAN
VPN
WAN

Default:

LAN

VPN

2.33.4.3 ISDN

The ISDN connections are configured over these lines. In addition to the physical ISDN line to be used, a telephone number translation is configured as well. This ensures the internal telephone number or SIP URL is converted to an external ISDN number.

Console path:

Setup > **Voice-Call-Manager** > **Lines**

2.33.4.3.1 Interfaces

This is where the lines to ISDN exchanges or PBX systems are configured (the router is the terminal device).

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

2.33.4.3.1.1 Name

This name uniquely identifies the line. It may not be assigned to any other line.

Here you can, for example, enter the telephone number for a group that is to receive incoming calls. This allows you to flexibly control which telephones ring for incoming calls, or to transfer calls to a mobile phone number or answering machine after a certain time.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.3.1.2 Ifc

From the available ISDN interfaces, select the ISDN interface that the ISDN subscribers are connected to.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

2.33.4.3.1.3 Domain

Domain in which the calls from/to the ISDN line are managed in the device's SIP world.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.3.1.4 Cln-Prefix

The call prefix is a number placed in front of the caller number (CLI; SIP "From:") for all incoming calls. This generates unique telephone numbers for return calls.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

Possible values:

Max. 9 characters from `[0-9]`

Default:

empty

2.33.4.3.1.5 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

Possible values:

No
Yes

Default:

Yes

2.33.4.3.1.6 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.3.2 Mapping

ISDN mapping assigns external ISDN telephone numbers (MSN or DDI) to the telephone numbers that are used internally. You can enter up to 64 telephone number assignments.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN**

2.33.4.3.2.1 MSN/DDI

This line's external telephone number in the ISDN network.

For incoming calls that are directed to this number, the corresponding internal telephone number is entered as the destination number. For outgoing calls, this number is transmitted as the caller's number, unless this has been suppressed.

MSN

Number of the telephone line

DDI (Direct Dialing in)

Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

Possible values:

Max. 19 characters from `[0-9]`

Default:

empty

2.33.4.3.2.2 Ifc

From the available ISDN interfaces, select the ISDN interface(s) used to connect the terminal equipment to the VoIP router. These line have to be configured as ISDN-NT.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

2.33.4.3.2.3 Number/Name

Internal telephone number of the ISDN telephone or name of the user (SIP URL).

For incoming calls, this is the SIP name or internal telephone number of the telephone to which the call from this interface is switched with the corresponding MSN/DDI. For outgoing calls, the SIP name is replaced by the MSN/DDI of the corresponding entry.

By using the # character as a placeholder, entire groups of call numbers, e.g. when using extension numbers, can be addressed via a single entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.4.3.2.4 CLIR

The display of your telephone number is suppressed so the person called cannot see it.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

Possible values:

No
Yes

Default:

No

2.33.4.3.2.5 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

Possible values:

No
Yes

Default:

Yes

2.33.4.3.2.6 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **ISDN** > **Mapping**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.4.4 Predef-Dest.

Table with predefined special functions for the destination lines in the call routing entries.

Console path:

Setup > **Voice-Call-Manager** > **Lines**

2.33.4.4.1 Name

Predefined special functions for the destination lines in the call routing entries.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **Predef-Dest.**

Possible values:

REJECT

Highlights a blocked telephone number.

USER

Forwards the call to local SIP, analog or ISDN subscribers.

RESTART

Starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

Default:

REJECT

USER

RESTART

2.33.4.5 Source filters

Table with predefined source lines to filter calls from local users.

Console path:

Setup > **Voice-Call-Manager** > **Lines**

2.33.4.5.1 Name

Predefined source lines to filter calls from local users.

Console path:

Setup > **Voice-Call-Manager** > **Lines** > **Source-Filters**

Possible values:

USER.ANALOG
For calls from a local analog subscriber.

USER.ISDN
For calls from a local ISDN subscriber.

USER.SIP
For calls from a local SIP subscriber.

USER#
For calls from a local subscriber in general.

Default:

USER.ANALOG

USER.ISDN

USER.SIP

USER#

2.33.5 Call router

This menu contains the call router settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

2.33.5.1 Call routing

Rules can be defined here for redirecting or rejecting calls to certain call targets or lines.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router**

2.33.5.1.1 Called ID

The called party name or destination telephone number (without domain information) that is called.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Special values:

#

The # character is used as a placeholder for any character strings. All characters in front of the # are removed, the remaining characters are used in the "Number/name" field instead of the # character to further establish the connection.

Example: The call routing table contains entry `00049#` as the called number/name and `00#` as the number/name. For all calls with a preceding '0' for outside-line access and the complete dialing code for Germany, only the leading '0' for the outside-line access and the leading '0' for the local area dialing code are retained as the number/name; the country ID is removed. For example, `00049 2405 123456` becomes `0 02405 123456`.

2.33.5.1.2 Cld-Domain

This entry filters the called domain, the "Called Party Domain". The call router entry is only considered to match if the Called Party Domain for the call matches the domain that is entered here. If nothing is specified, any destination domain is accepted.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Analog
ISDN
The internal VoIP domains of the VoIP router.
All domains entered for the SIP and SIP-PBX lines.

2.33.5.1.3 Calling ID

This entry filters the calling number/name, the "calling party ID". It is specified as an internal number or as a national or international telephone number. The domain is not specified. No "0" or other character for a line ID is prefixed; the ID is used as if it comes from the line or from internal telephone calls.

The call router entry is only evaluated as matching if the Calling Party ID for the call matches the number that is entered here. After "#", any characters can be accepted.

If nothing is specified here, any Calling Party ID is accepted.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Internal number
National telephone number
International telephone number
LOCAL

Restricts to internal telephone numbers (without a leading "0").

EMPTY

Optional for unspecified Calling Party IDs.

2.33.5.1.4 Cld-Domain

This entry filters the "calling domain". The call router entry is only considered to match if the Calling Domain for the call matches the domain that is entered here. If nothing is specified, each calling domain is accepted.

SIP telephones usually have several line keys, for which different domains can be configured. With this filter, telephone calls are handled depending on the selection that is made using different line keys.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Analog
ISDN
The internal VoIP domains of the VoIP router.
All domains entered for the SIP and SIP-PBX lines.

2.33.5.1.5 Src-Line

This entry filters the source line. The call router entry is only considered to match if the source line for the call matches the line that is entered here. If nothing is specified, any calling line is accepted.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

USER.ANALOG

For calls from a local analog subscriber.

USER.ISDN

For calls from a local ISDN subscriber.

USER.SIP

For calls from a local SIP subscriber.

USER#

For calls from a local subscriber in general.

All ISDN, SIP and SIP-PBX lines that are entered.

2.33.5.1.7 Dest-Id-1

This entry filters the source line. The call router entry is only considered to match if the source line for the call matches the line that is entered here. If nothing is specified, any calling line is accepted.

At least one of the entries "Number/Name", "1st Backup No." or "2nd Backup No." must be filled in. They are evaluated in this sequence. A blank field is skipped.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.5.1.8 Dest-Line-1

The connection is established using the destination line.

This field has to be completed, otherwise the entry is not used.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Analog
ISDN
All defined SIP lines.
REJECT
Highlights a blocked telephone number.
USER
Forwards the call to local SIP, analog or ISDN subscribers.
RESTART
Starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

2.33.5.1.9 Active

The routing entry can be activated, deactivated, or marked as a default entry. All calls that can be resolved using the first passes but not using the call routing table or local subscriber table are then automatically resolved using these default entries. You can use any destination name and destination domain; only any source filters that you have set will be processed.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Active
No
Default line

Default:

Active

2.33.5.1.10 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.5.1.11 Dest-Id-2

This telephone number is used to establish the connection further if nothing is entered in "number/name" or the corresponding "line" is not available. If no connection can be established using this 2nd call number and the relevant 2nd line, the 3rd call number and 3rd line will be used.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.5.1.12 Dest-Line-2

The connection is established using this line if the 2nd number is used to establish the connection. The same lines can be dialed as for "line".

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Analog
ISDN
All defined SIP lines.
REJECT
Highlights a blocked telephone number.
USER
Forwards the call to local SIP, analog or ISDN subscribers.
RESTART
Starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

2.33.5.1.13 Dest-Id-3

Similar to the 2nd number.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.5.1.14 Dest-Line-3

Similar to the 2nd line.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Analog
ISDN
All defined SIP lines.
REJECT
Highlights a blocked telephone number.
USER
Forwards the call to local SIP, analog or ISDN subscribers.
RESTART
Starts a new pass through the call routing table with the previously formed "number/name". The former "source line" is deleted.

2.33.5.1.15 Prio

The Call Manager sorts all entries with the same priority automatically, so that the table can be processed through logically from top to bottom. With some entries, however, the sequence of the entries has to be specified (for the telephone number translation, for example). The entries with the highest priority are automatically sorted to the top.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

0 … 999

Default:

0

2.33.5.1.16 Dest-Calling-Id

If the calling number is to be replaced by another number in the call route, the desired number must be entered in this field. If the special value "EMPTY" is entered and the filter field *2.33.5.1.1 Called ID* on page 1131 is filled with any character (e.g. wildcard #) at the same time, a number suppression for outgoing calls can be configured for the call route.

Console path:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Possible values:

Max. 38 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default:

empty

2.33.7 Groups

This menu contains the user-group settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

2.33.7.1 Groups

Groups are defined here that enable incoming calls to be automatically distributed to two or more subscribers.

Console path:

Setup > **Voice-Call-Manager** > **Groups**

2.33.7.1.1 Name

The hunt group is available under this telephone number or SIP-ID.

The names of hunt groups may not coincide with the names of users (SIP, ISDN, analog).

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.7.1.2 Members

Comma-separated list of the members of the hunt group. Members can be users, hunt groups or external telephone numbers, and so there is no limit on scaling.

A hunt group may not contain itself or any parents in the hierarchical system—recursion through member entries is not possible. However, loops to parents in the structure may result from the "forwarding target".

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

Users
Hunt groups
External telephone numbers

2.33.7.1.3 Distribution method

Sets the type of call distribution.

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

Simultaneous

The call is signaled to all group members at once. If a member picks up the call within the call-forwarding time, the call is no longer signaled to other group members. If nobody accepts the call within the forwarding time, then the call is switched to its forwarding destination.

Sequential

The call is directed to one member of the group after the other. If a group member does not accept the call within the forwarding time, then the call is switched to the next member of the group. If nobody in the group accepts the call within the forwarding time, then the call is switched to its forwarding destination.

Default:

Simultaneous

2.33.7.1.4 Forwarding time

If an incoming call is not picked up by a group member within the forwarding time, then the call is forwarded according to the distribution method selected:

In the case of simultaneous call distribution, the call is forwarded to the forwarding destination.

In case of sequential call distribution, the call is forwarded to the next group member in line. If the group member is the last one in the sequence, then the call is redirected to its forwarding destination.

If all members of the group are busy or unavailable, then the call is redirected to the forwarding destination without waiting for the forwarding-time to expire.

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

0 … 255 Seconds

Default:

0

Special values:

0

The call is forwarded immediately to the forwarding destination (temporarily jumps a hunt group in a hierarchy).

2.33.7.1.5 Forwarding target

If none of the group members accepts the call within the forwarding time, then the call is switched to the forwarding destination entered here. Forwarding destinations can be users, hunt groups or external telephone numbers. Only one forwarding destination can be entered.

The forwarding target only becomes active once the group's forwarding time has expired or if no members are available. Here, too, redirection to a higher level of the hunt-group structure is possible, unlike with the "Members" entry.

If no forwarding target is defined, then the call is rejected as soon as the member list has been worked through, or if all members are busy or unavailable.

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

Users
Hunt groups
External telephone numbers

2.33.7.1.6 Active

Activates or deactivates the entry.

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

No
Yes

Default:

Yes

2.33.7.1.7 Comment

Comment on this entry.

Console path:

Setup > **Voice-Call-Manager** > **Groups** > **Groups**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.8 Logging

This menu contains the logging settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager**

2.33.8.1 Call-Data-Records

This menu contains the logging settings for the Call Manager.

Console path:

Setup > **Voice-Call-Manager** > **Logging**

2.33.8.1.1 E-mail notification

You can optionally receive information about all of the calls made via the VoIP router via e-mail. For every call which is connected (internal, external, incoming, outgoing), a message is generated containing information such as the source and target number, start-time and end-time of the call, etc.

An SMTP account has to be configured in order to use messaging via e-mail.

Console path:

Setup > **Voice-Call-Manager** > **Logging**

Possible values:

No
Yes

Default:

No

2.33.8.1.2 E-mail address

E-mail address for sending messages.

Console path:

Setup > **Voice-Call-Manager** > **Logging**

2.33.8.1.3 Syslog

You can also obtain information on all calls made over the VoIP router using SYSLOG (facility: accounting; level: info). For every call which is connected (internal, external, incoming, outgoing), a message is generated containing information such as the source and target number, start-time and end-time of the call, etc.

A syslog client must be set up to make use of this function.

Console path:

Setup > **Voice-Call-Manager** > **Logging**

Possible values:

No
Yes

Default:

No

2.33.10 DECT

This menu contains the configuration options for DECT base stations and DECT handsets.

Console path:

Setup > **Voice-Call-Manager**

2.33.10.1 Base stations

This entry is used to configure your DECT base stations.

Console path:

Setup > **Voice-Call-Manager** > **DECT**

2.33.10.1.1 Name

Specify a unique name for this base station here.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Max. 15 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.33.10.1.2 MAC address

Enter the MAC address of the base station.

If you wish to permit communications with any MAC address, enter `000000000000`.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Max. 17 characters from `[a-f][0-9]`

Default:

000000000000

2.33.10.1.4 Routing tag

This entry shows the routing tag used.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.33.10.1.5 Remote-Configuration

By default, a DECT 510 does not allow access to the configuration from remote networks.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

No

Remote configuration not allowed.

Yes

Remote configuration allowed.

Default:

No

2.33.10.1.6 Frequency-Band

Here, the DECT frequency band of a Gigaset N670 or N870 base station can be set during provisioning.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Unchanged

The frequency band configured in the base station is not changed.

Europe
Setting for Europe.

Latin-America
Setting for Latin-America.

Brazil
Setting for Brazil.

Default:

Unchanged

2.33.10.1.7 Admin-Password

Here you can set the administrator password of a Gigaset N670 or N870 base station during provisioning.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Min. 8 and max. 40 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Special values:

empty
If the entry is empty, no password is transmitted in the XML. Thus, the password set so far remains unchanged.

Default:

empty

2.33.10.2 Handsets

This entry is used to configure your DECT handsets.

Console path:

Setup > **Voice-Call-Manager** > **DECT**

2.33.10.2.1 Base station name

Here you select the base station where the corresponding handset is registered.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 15 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

DEFAULT

2.33.10.2.2 Index

Enter here the number of the corresponding handset (e.g. "0" for handset 1, "1" for handset 2).

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

0 … 6

Default:

0

2.33.10.2.3 SIP user

Select the phone number of the handset here.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 20 characters from `[0-9]+-`

Default:

empty

2.33.10.2.4 Handset name

Here you set the name to be shown in the display of the handset.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.33.10.2.5 Display name

Here you set the name to be sent to a caller.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.10.2.6 Voice mailbox

Enter the phone number of your voice mailbox here. This phone number is dialed by pressing and holding the button "1" on the handset.

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 20 characters from `[0-9]+-`

Default:

empty

2.33.10.2.7 Handset-ID

Enter the handset ID (IUID) of the respective handset here.When using the LANCOM DECT N510 IP, enter the number of the respective handset (e.g. “0” for handset 1, “1” for handset 2).

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 10 characters from `[0-9a-f]`

Default:

0

2.33.11 SIP server

This menu contains the configuration settings for the SIP server.

Console path:

Setup > **Voice-Call-Manager**

2.33.11.1 TLS server

Use this menu to configure the TLS server for the encryption of the SIP connections.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server**

2.33.11.1.1 Operating

This entry is used to enable or disable the TLS server.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

No
Yes

Default:

Yes

2.33.11.1.2 Port

Use this entry to define the TLS-server port to be used for establishing an encrypted connection.

This port has to be activated in the firewall for the connection to work.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

No
Yes

Default:

Yes

2.33.11.1.10 Versions

Here you select the encryption version(s) to be used.

All versions are selected by default.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

TLSv1
TLSv1.1
TLSv1.2

2.33.11.1.11 Key-exchange algorithms

Here you select the encryption version(s) to be used.

All versions are selected by default.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

RSA
DHE
ECDHE

2.33.11.1.12 Crypto-Algorithms

Here you select the encryption algorithms to be used.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.33.11.1.13 Hash algorithms

Here you select the hash algorithms to be used.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

MD5
SHA1
SHA-256
SHA-384
SHA2-256
SHA2-384

Default:

SHA1

SHA-256

SHA-384

SHA2-256

SHA2-384

2.33.11.1.14 Prefer PFS

Specify whether PFS (perfect forward secrecy) is enabled for the SSL/TLS secured connection.

To disable this function, uncheck the box.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

Yes

Default:

Yes

2.33.11.1.15 Renegotiations

Specify whether new negotiations are permitted for secure connections.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

Forbidden
Allowed
Ignored

Default:

Allowed

2.33.11.1.16 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

All entries are selected by default.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

secp256r1
secp384r1
secp521r1

2.33.11.1.30 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

All algorithms are selected by default.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server** > **TLS-Server**

Possible values:

SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

2.33.11.2 UDP server operating

Use this entry to enable or disable the UDP server.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server**

Possible values:

No
Yes

Default:

Yes

2.33.11.3 UDP server port

Use this entry to specify the server port for UDP connections.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server**

Possible values:

0 … 65535

Default:

5060

2.33.11.4 TCP server operating

Use this entry to enable or disable the TCP server.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server**

Possible values:

No
Yes

Default:

Yes

2.33.11.5 TCP server port

Use this entry to specify the server port for TCP connections.

Console path:

Setup > **Voice-Call-Manager** > **SIP-Server**

Possible values:

0 … 65535

Default:

5060

2.33.12 Call-Handling

This menu contains the settings for call handling.

Console path:

Setup > **Voice-Call-Manager**

2.33.12.1 Preferred-Numbers

Enter your preferred phone numbers here and enter your comments.

Console path:

Setup > **Voice-Call-Manager** > **Call-Handling**

2.33.12.1.1 Called-Number

Enter your telephone number here.

Console path:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Possible values:

20 characters from: `[0-9]+-`

2.33.12.1.2 Type

Enter the call number types.

Console path:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Possible values:

Landline
Mobile
Fax

Default:

Landline

2.33.12.1.4 Comment

Here you enter a comment on the selected number.

Console path:

Setup > **Voice-Call-Manager** > **Call-Handling** > **Preferred-Numbers**

Possible values:

Characters from the following character set:
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.33.12.2 RTP-Threshold

Here you set the RTP threshold in milliseconds.

Console path:

Setup > **Voice-Call-Manager** > **Call-Handling**

Possible values:

0 … 780000

Default:

50

2.34 Printer

This menu contains settings for the printer.

Console path:

Setup

2.34.1 Printer

You can adjust setting for the network printer here.

Console path:

Setup > **Printer**

2.34.1.1 Printer

Printer name.

Console path:

Setup > **Printer** > **Printer**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

*

2.34.1.2 RawIp-Port

This port can be used to accept print jobs over RawIP.

Console path:

Setup > **Printer** > **Printer**

Possible values:

Max. 10 characters from `[0-9]`

Default:

9100

2.34.1.3 LPD port

This port can be used to accept print jobs over LDP.

Console path:

Setup > **Printer** > **Printer**

Possible values:

Max. 10 characters from `[0-9]`

Default:

515

2.34.1.4 Operating

Activates or deactivates this entry.

Console path:

Setup > **Printer** > **Printer**

Possible values:

No

The print server is not active.

Yes

The print server is active.

Default:

No

2.34.1.5 Bidirectional

This parameter enables or disables the bi-directional mode of the printer.

The bidirectional model of the printer is intended exclusively for development and support purposes. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **Printer** > **Printer**

Possible values:

No

The print server is not active.

Yes

The print server is active.

Default:

No

2.34.1.6 Reset-on-Open

If this option is activated the device will send a reset command to the printer before opening a printer session.

Activate this option if the connection to the printer does not work as expected.

Console path:

Setup > **Printer** > **Printer**

Possible values:

No
Yes

Default:

No

2.34.2 Access list

Here you define the networks that have access to the printer.

Console path:

Setup > **Printer**

2.34.2.1 IP address

IP address of the network with clients requiring access to the printer.

Console path:

Setup > **Printer** > **Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.34.2.2 IP-Netmask

Netmask of the permitted networks.

Console path:

Setup > **Printer** > **Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.34.2.3 Rtg-Tag

If you specify a routing tag for this access rule, the only packets that will be accepted have received the same tag in the firewall or they are from a network with the corresponding interface tag.

It follows that the use of routing tags only makes sense in combination with the appropriate rules in the firewall or tagged networks.

Console path:

Setup > **Printer** > **Access-List**

Possible values:

Max. 5 characters from `[0-9].`

Default:

0

Special values:

0

Access attempts from approved IP addresses are accepted every time.

2.37 WLAN-Management

This menu is used to configure WLAN management for WLCs.

Console path:

Setup

2.37.1 AP-configuration

This menu contains the settings for the AP.

Console path:

Setup > **WLAN-Management**

2.37.1.1 Network-profiles

Here you define the logical WLAN networks that can be activated and operated on the associated APs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.1.1 Name

Name of the logical WLAN network under which the settings are saved. This name is only used for internal administration of logical networks.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.1.2 Parent name

A WLC is capable of managing a wide range of different APs at different locations. However, WLAN profiles include settings that are not equally suitable for every type of AP that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for different countries or device types, it is possible for the logical WLAN networks to "inherit" properties from other entries.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.1.3 Local values

Specifies which logical wireless LAN parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 12 characters from `[0-9]`

Default:

000000000000

2.37.1.1.4 Operating

Switches the logical WLAN on or off separately.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No
Yes

Default:

Yes

2.37.1.1.6 Encryption

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Please consider that not all wireless cards support all encryption methods.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

802.11i-WPA-PSK
802.11i-WPA-802.1x
WEP-104-Bit
WEP-40-Bit
WEP-104-Bit-802.1x
WEP-40-Bit-802.1x
None
Enhanced-Open
Enhanced-Open-Transitional

Default:

802.11i-WPA-PSK

2.37.1.1.7 WPA1-Session-Keytypes

Here you select the methods which are to be made available for generating WPA session keys and group key. There is a choice of the Temporal Key Integrity Protocol (TKIP), the Advanced Encryption Standard (AES), or both.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

TKIP/AES
AES
TKIP

Default:

TKIP/AES

2.37.1.1.8 WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default:

WPA2

2.37.1.1.9 Key

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "0x". The following lengths result for the formats used: Method, length WPA-PSK 8-63 ASCII characters WEP152 (128 bit) 16 ASCII or 32 HEX characters WEP128 (bit 104) 13 ASCII or 26 HEX characters WEP64 (bit 40) 5 ASCII or 10 HEX characters

Console path:

Setup > **WLAN-Management** > **Networkprofiles**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.1.10 Radio-Band

Selecting the frequency band determines whether the wireless LAN adapter operates in the 2.4 GHz, 5 GHz or 6 GHz band, which in turn determines the available radio channels.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

All
2.4GHz
5GHz
6GHz

Default:

All

2.37.1.1.11 Continuation

The time in minutes that a managed-mode AP continues to operate in its current configuration.

The configuration is provided to the AP by the WLC and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLC be interrupted, the AP will continue to operate with the configuration stored in flash for the time period entered here. The AP can also continue to work with this flash configuration after a local power outage.

If there is still no connection to the WLC after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLC can be reached again, the configuration is transmitted again from the WLC to the AP.

This option enables an AP to continue operating even if the connection to the WLC is temporarily interrupted. Furthermore this represents an effective measure against theft as all security-related configuration parameters are automatically deleted after this time has expired.

All other WLAN network parameters correspond to those for the standard configuration of APs.

If the AP establishes a backup connection to a secondary WLC then the countdown to the expiry of standalone operation is halted. The AP and its WLAN networks remain active as long as there is a connection to a WLAN controller.

Please note that the configuration in flash memory is deleted only after expiry of the time for standalone operation, and not when the power is lost!

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 9999

Default:

0

Special values:

0

Switches the WLAN module off the moment that the connection to the Controller is lost. With this setting, the configuration provided by the WLC is not stored in flash memory but in RAM, meaning that a power outage causes the configuration to be lost immediately.

9999

Continues working indefinitely with the current configuration, even if the WLAN controller is permanently unavailable. The WLAN configuration in the flash memory is only deleted after a reset.

2.37.1.1.12 Min-Tx-Rate

Normally the AP negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The AP adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum transmission speed if you wish to prevent the dynamic speed adjustment.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
T-72M
T-96M
T-108M

Default:

Auto

2.37.1.1.13 Max-Tx-Rate

Normally the AP negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The AP adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed value for the maximum transmission speed if you wish to prevent the dynamic speed adjustment.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
T-72M
T-96M
T-108M

Default:

Auto

2.37.1.1.14 Basic rate

The defined broadcast rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster".

If you select “Auto” here, the device automatically depends on the transmission rate of the slowest WLAN client in the network.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
T-72M
T-96M
T-108M

Default:

Auto

2.37.1.1.15 11b-Preamble

Normally, the clients in 802.11b mode negotiate the length of the preamble with the AP. "Long preamble" should only be set when the clients require this setting to be fixed.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
Long

Default:

Auto

2.37.1.1.16 MAC filter

The MAC addresses of the clients allowed to associate with an AP are stored in the MAC filter list. The **MAC filter** switch allows the use of the MAC filter list to be switched off for individual logical networks.

Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The MAC filter list is always consulted for registrations with an individual passphrase, even if this option is deactivated.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

No

2.37.1.1.17 Cl.-Brg.-Support

Whereas address adaptation allows only the MAC address of a single attached device to be visible to the AP, client-bridge support provides transparency in that all MAC addresses of the LAN stations behind the client stations are transferred to the AP.

Furthermore, the three MAC addresses usual in client mode are not used for this operating mode (in this example for server, AP and client station), but rather four addresses as with point-to-point connections (the fourth is the MAC address of the station in the LAN of the client station). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, initiated by a broadcast.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No

Deactivates client-bridge support for this logical WLAN.

Yes

Activates client-bridge support for this logical WLAN.

Exclusive

Only accepts clients that also support the client-bridge mode.

Default:

No

2.37.1.1.18 Max. stations

Here you set the maximum number of clients that may associate with this AP. Additional clients wanting to associate will be rejected.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 65535

Default:

0

2.37.1.1.19 SSID broadcast (WLCs only)

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated on the AP, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the AP, this transmits the SSID in cleartext so that it is briefly visible to all clients in the WLAN network.

The "closed network" function for the AP is to be found under **Setup** > **Interfaces** > **WLAN** > **Network**. Please note: If the WLC has the option **SSID broadcast** set to "No" (device does not broadcast the SSID), the AP sets its **closed network** option to "Yes", and vice versa. Only with the setting "Tightened" do both devices retain identical settings.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No

The AP does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the AP similarly responds with an empty SSID.

Yes

The AP publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the AP responds with the SSID of the radio cell (publicly visible WLAN).

Tightened

The AP does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the AP does not respond.

Default:

Yes

2.37.1.1.21 SSID

Define a unique SSID (the network name) for each of the logical wireless LANs required. Only WLAN clients that have the same SSID can register with this wireless network.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.1.22 Min.-HT-MCS

A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i.e. proportion of error correction bits in the raw data) and number of spatial streams. 802.11n uses this term instead of the term "data rate" used in older wireless LAN standards because data rate is no longer an unambiguous description.

Selecting the MCS therefore specifies the minimum and maximum modulation parameters to be used. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput. You can find a list with the values for the different MCS in the reference manual.

The first digit specifies the modulation parameters for one spatial stream, the second digit specifies the modulation parameters for two spatial streams.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

2.37.1.1.23 Max.-HT-MCS

A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i.e. proportion of error correction bits in the raw data) and number of spatial streams. 802.11n uses this term instead of the term "data rate" used in older wireless LAN standards because data rate is no longer an unambiguous description.

Selecting the MCS therefore specifies the minimum and maximum modulation parameters to be used. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput. You can find a list with the values for the different MCS in the reference manual.

The first digit specifies the modulation parameters for one spatial stream, the second digit specifies the modulation parameters for two spatial streams.

In the default setting the station automatically selects the best possible MCS for each stream, based on the conditions of each channel. If interference arises during operation and the channel conditions change, for example

due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

2.37.1.1.24 Short guard interval

This option is used to reduce the transmission pause between two signals from 0.8 s (default) to 0.4 s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode provided the operating conditions allow this. Alternatively the short guard mode can be switched off.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
No

Default:

Auto

2.37.1.1.25 Max-Spatial-Streams

The spatial multiplexing function allows several separate data streams to be transmitted over separate antennas in order to increase data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

With the "Auto" setting all spatial streams that are supported by the wireless LAN module in question are used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
One
Two
Three
Four

Default:

Auto

2.37.1.1.26 Send-Aggregates

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This method serves to reduce the packet overhead, and the data throughput increases.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

Yes

2.37.1.1.28 RADIUS accounting activated

Enables or disables the RADIUS accounting on this logical WLAN network.

The APs supporting the logical WLAN network as configured by the WLC must have a LCOS firmware version 8.00 or higher.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

No

2.37.1.1.30 VLAN mode

This item allows you to select the VLAN mode for this WLAN network (SSID).

The AP only uses the VLAN settings for the logical WLAN if you activate the VLAN module in the AP (in the physical WLAN parameters). The setting "untagged" for a specific WLAN allows you to operate in a wireless LAN without VLAN, even if VLAN is otherwise activated.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

tagged
The AP marks the packets of this SSID with the ID configured under *2.37.1.1.34 VLAN-ID* on page 1170.

untagged
The AP forwards the packets of this SSID without any VLAN ID.

Default:

untagged

2.37.1.1.32 Connect-SSID-to

Here you can select the logical interface used by the AP to transfer the payload data from this WLAN network (SSID).

Forwarding payload data from multiple SSIDs to the WLC increases the CPU load and bandwidth demands of the central devices. Consider the performance requirements of central WLAN management that uses layer-3 tunneling.

For each AP you can connect up to 7 SSIDs with a WLC tunnel. For each AP, the WLC connects the WLC tunnel and its associated SSID to an available bridge group. Since one of the eight available bridge groups is reserved for other purposes, 7 bridge groups remain for assigning the WC-tunnel.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

LAN

The AP forwards payload data from this WLAN network via the bridge to its own local LAN interface. In this case, configure how the data packets are to be further processed by using appropriate routes directly on the AP, for example through a separate Internet connection.

WLC-Tunnel-1 ... WLC-Tunnel-x (depending on the model)

The AP forwards the payload data from this WLAN network via one of the virtual interfaces to the WLC (WLC tunnel). In this case, configure how the data packets are to be further processed by using appropriate routes centrally on the WLC, for example through a shared Internet connection.

L2TP-ETHERNET-1 … L2TP-ETHERNET-x (depending on the model)

The SSID is connected to an L2TPv3-Ethernet tunnel. This enables the automatic break-out of WLAN SSIDs through L2TP-Ethernet tunnels. L2TPv3 tunnels are recommended as an alternative to the classic WLC layer-3 tunnel if the latter limits the WLAN throughput. Higher maximum throughputs can be achieved with L2TPv3. Then adjust the usage of the L2TP-ETHERNET-x interface used on the WLC, e.g. for further use on the IP router or LAN bridge.

Default:

LAN

2.37.1.1.33 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. The setting that decides whether clients within an SSID can exchange data with one another has to be set separately for each logical WLAN.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

Yes

2.37.1.1.34 VLAN-ID

This item allows you to set the VLAN ID for this logical WLAN network. When the VLAN mode is set to "tagged", the AP transmits the data from this WLAN network (SSID) with the VLAN ID set here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

2 … 4094

Default:

2

2.37.1.1.35 RADIUS profile

Here you enter the name of the RADIUS profile containing the information about the RADIUS server used for the authentication of the user data and the accounting of user activity.

SNMP ID: 2.37.1.1.35

Telnet path:/Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

› Max. 16 characters

Default: Blank

2.37.1.1.36 STBC-activated

STBC is an encoding method according to IEEE 802.11n. The "STBC" (Space Time Block Coding) function varies the transmission of data packets over time in addition to space to minimize temporal effects on the data. The temporal offset of transmissions provides the receiver with an even better chance of receiving error-free data packets, regardless of the number of antennas. This results in improved reception conditions in a MIMO system.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No
Yes

2.37.1.1.37 LDPC activated

With this setting you enable LDPC for the corresponding logical network. LDPC (Low Density Parity Check) is a method to correct errors during data transmission. If you do not enable LDPC, your device uses the less effective Convolution Coding (CC) method which is defined for error correction in the IEEE 802.11n standard.

APs in your network that do not support LDPC ignore this setting.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No
Yes

Default:

Yes

2.37.1.1.38 Min-Client-Strength

A WLAN installation at a location with a really large potential number of clients (e.g., a football stadium) has considerable throughput problems. In this type of scenario, a possible cause is a large percentage of overhead due to remote stations with a weak connection. If one of these stations is registered (associated), the access point can only send data to this station with a relatively low physical bit-rate – possibly with several repetitions per packet. Not only does this result in a weak connection for the user, it also places a load on the medium to the detriment of clients with stronger connections, which would otherwise make more effective use of the available bandwidth. It should be noted that unregistered remote stations can also negatively impact the throughput of the cell when attempting to find a network. Probe requests (search packets) of such clients must be directly and specifically answered by the AP after reception, e.g., they will be repeated until the client has confirmed receipt or the maximum number of repetitions is reached. The effect is worsened by the fact that these response packets are WLAN management packets, which are usually transmitted at the lowest available fixed bit rate as supported by the AP.

Although there is no way that an AP can prevent clients from sending probe requests, it can ignore them or simply not respond to them if they fall below a certain signal strength.

A configured **Min-Client-Strength** functions as follows:

- If a probe request with an appropriate SSID or a placeholder SSID is received, a response is only sent if it has at least the minimum signal strength. If not, it is silently discarded.
- If an authentication or registration request is received, which is below the configured signal strength, it will be rejected. Please note that this situation is rare, since the probe requests of such clients usually go unanswered anyway, and a client can only have found this AP using a passive search of its radio beacon.

This value is specified as a percentage. This specifies the ratio of the signal and noise levels (SNR). A percentage value of 100% means an SNR of 64 dB, smaller percentage values are correspondingly lower. The default value is 0, e.g., no clients are ignored.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 255

Default:

0

2.37.1.1.39 IEEE802.11u-Network-Profile

Using this parameter you specify the name given under **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles** of an 802.11u network profile, which is to be assigned to the logical wireless network.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.1.40 OKC

With opportunistic key caching, the management of WLAN client keys is moved to a WLC or central switch, which manages all of the APs in the network. When a client authenticates at an AP, the downstream WLC, which acts as the authenticator, performs the key management and returns the PMK to the AP for forwarding to the client. If the client moves to another cell, it uses this PMK and the MAC address of the new AP to calculate a PMKID, and it sends this to the new AP in the expectation that OKC is enabled (i.e. "opportunistic"). If the AP is unable to handle the PMKID, it negotiates a regular 802.1X authentication with the client.

An AP is even able to perform OKC if the WLC is temporarily unavailable. In this case it stores the PMK and sends it to the WLC, once available again. The WLC then sends the PMK to all of the AP in the network so that the client can continue to use OKC when moving between cells.

With this setting you enable OKC on the AP which is to be managed by the WLC.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No
Yes

Default:

Yes

2.37.1.1.41 WPA2 key management

You configure the WPA2 key management with these options.

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the AP are compatible. Unsuitable clients may refuse a connection if an option other than **Standard** is enabled.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Fast roaming
Enables fast roaming as per 802.11r

SHA256
Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

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.

Default:

Standard

2.37.1.1.42 APSD

Activates APSD power saving for the corresponding logical WLAN network.

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

Yes

2.37.1.1.43 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 AP. 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, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No
The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory
The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional
The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

2.37.1.1.44 Tx-Limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

2.37.1.1.45 Rx-Limit

With this setting, you define the overall bandwidth that is available for reception within this SSID.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

2.37.1.1.46 LBS-Tracking

This option specifies whether the LBS server is permitted to track the client information.

This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Yes
No

Default:

No

2.37.1.1.47 LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **LBS-Tracking**

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.1.49 11ac-Beamforming

Here you configure the 11ac-Beamforming.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Auto
No
SU-MIMO
MU-MIMO

2.37.1.1.50 Convert-to-Unicast

You have these options for converting data streams into Unicast. DHCP and Multicast can also be selected together.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

None

No data streams are converted into Unicast.

DHCP

Converts DHCP server response messages into Unicast if the server has sent them as Broadcast. This increases the reliability of delivery because data packets sent as Broadcast have no specific recipient, no optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and a low data rate.

Multicast

Multicast data streams that are to be transmitted over WLAN interfaces are converted into individual Unicast data streams per client on the MAC layer or WLAN layer when this feature is activated. Although the packets are duplicated per client, they can now be transmitted at the highest possible data rate for that client since they are now Unicasts. Even though packets are duplicated, the much faster transmission generally uses significantly less airtime in most scenarios, leaving more airtime available for other transmissions.

For this feature to work, IGMP snooping must be enabled and properly configured on the device. Using IGMP snooping, the device determines which client wants to receive which multicast stream. This provides the multicast conversion with the appropriate target clients or addresses for the conversion.

2.37.1.1.51 Transmit-only-Unicasts

Multicast and broadcast packets forwarded into a WLAN cell can consume a significant portion of the media bandwidth in that cell. Even if an access point (AP) employs optimization techniques such as ARP spoofing, IGMP/MLD snooping, or dynamic adjustment of the multicast bit rate, the fact remains that the majority of multicast and broadcast traffic in a congested core network is completely useless to the clients.

Assuming no multicast streaming to clients is desired, ARP requests are answered by the AP itself. Conversely, if pure IPv4 internet access is to be provided, it is possible to operate entirely without forwarding broadcast or multicast traffic into a WLAN cell – the AP can simply filter them out. IPv4 broadcast and multicast traffic associated with self-learning protocols such as Bonjour or NetBIOS is generally undesirable in networks intended to provide public internet access.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

No

Broadcasts and multicasts are forwarded into this WLAN network.

Yes

Broadcasts and multicasts are not forwarded into this WLAN network.

Default:

No

2.37.1.1.52 Continuation-Time-use-default

If the autonomous continued operation for WLAN networks is configured on the WLC in such a way that networks are broadcast permanently (value: 9999), this also applies to locally at the LAN coupled networks, as well as for via WLC tunnel connected networks. In the event of a failure of the WLC, both types of networks are broadcast further; This only makes sense for networks connected via LAN, because via WLC tunnel the endpoint in the form of the WLC is missing and the networks are therefore not operational.

With this switch the two types of networks will be handled separately.

- If the switch is set, locally decoupled networks will continue to operate autonomously and permanently. Networks decoupled via a WLC tunnel, on the other hand, are only broadcast if the WLC is accessible.
- If the switch is not set, the time specified under **Continuation** is used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

yes
no

Default:

no

2.37.1.1.53 WPA2-3-Session-Keytypes

Here you select the methods that users should be offered to generate the WPA session or group keys. The following Advanced Encryption Standard (AES) methods can be offered.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

AES-CCMP-128
TKIP
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default:

AES-CCMP-128

2.37.1.1.54 WPA 802.1X security level

Setting the 802.1X security level. WPA3 features the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments.

Operating CNSA Suite B cryptography requires the use of certain cipher suites. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP128 is also enforced with “Suite B 128 bits”.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Default

Suite-B 128-bit

Enabled “Suite B 128 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Suite-B 128-bit

Enabled “Suite B 192 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Default:

Default

2.37.1.1.55 Per-Client-Tx-Limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

2.37.1.1.56 Per-Client-Rx-Limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

2.37.1.1.57 Timeframe

Select one of the time frames defined in *2.37.1.26 Timeframe* on page 1286. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.1.58 Min-Client-Disassoc-Strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value *2.37.1.1.38 Min-Client-Strength* on page 1172 is also set and the Min-Stations-Disassoc-Strength is less than this value.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

0 … 100

Default:

0

2.37.1.2 Radioprofiles

Here you define the physical WLAN parameters which apply to all of the logical WLAN networks that share a managed AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.2.1 Name

Unique name for this combination of physical WLAN parameters.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.2.2 Parent-Name

A WLC is capable of managing a wide range of different APs at different locations. However, WLAN profiles include settings that are not equally suitable for every type of AP that can be managed. For rexample, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for different countries or device types, it is possible for the physical WLAN parameters to "inherit" properties from other entries.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.2.3 Local-Values

Specifies which physical wireless LAN parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Max. 6 characters from `[0-9]`

Default:

000000

2.37.1.2.4 Country

The device needs to be set with the country where it is operating in order for the WLAN to use the parameters approved for the location.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

default

Makes use of the encryption method defined in the 'Options' area.

Albania
Argentina
Australia
Austria
Bahrain
Bangladesh
Belarus
Bosnia-Herzegovina
Brazil
Brunei Dar es Salaam
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Croatia
Cyprus
Czech Republic
Denmark
Ecuador
Egalistan
Egypt
Estonia
Finland
France
Germany
Ghana
Greece
Guatemala
Honduras
Hong-Kong
Hungary
Iceland
India
Indonesia
Ireland
Israel
Italy
Japan
Jordan
South Korea
Latvia
Lebanon
Liechtenstein
Lithuania
Luxembourg
Macao
Macedonia
Malaysia
Malta
Mexico
Moldavia
Morocco

Netherlands
New Zealand
Nicaragua
Norway
Oman
Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Puerto Rico
Qatar
Romania
Russia
Saudi Arabia
Singapore
Slovakia
Slovenia
South Africa
Spain
Sweden
Switzerland
Taiwan
Tanzania
Thailand
Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
Great Britain
United States FCC
Uruguay
Venezuela

Default:

default

2.37.1.2.6 2.4GHz-Mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 2.4 GHz frequency band. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

11bg mixed
802.11g/b (mixed)

11b-only
802.11b only (11Mbps)

11g-only
802.11g only (54Mbps)

108Mbps
802.11g++ (108Mbps mode / Turbo mode)

11bgn mixed
802.11g/b/n

11gn mixed
802.11g/n

Greenfield
802.11n only (greenfield mode)

11bgnax-mixed
802.11g/b/n/ax

11gnax-mixed
802.11g/n/ax

11bgnaxbe-mixed
802.11g/b/n/ax/be

11gnaxbe-mixed
802.11g/n/ax/be

Auto
Automatic. In the 2.4 GHz mode, automatic selection provides either **11bgn-mixed** or **11bg-mixed**.

Default:

Auto

2.37.1.2.7 5GHz-Mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 5 GHz frequency band. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Normal
802.11g (54Mbps mode)

108Mbps
802.11g++ (108Mbps mode / Turbo mode)

11an mixed
802.11a/n (mixed)

Greenfield
802.11n only (greenfield mode)

11anac mixed
802.11a/n/ac (mixed)

11nac mixed
802.11n/ac (mixed)

11ac-only
802.11ac only

11anacax-mixed
802.11a/n/ac/ax (mixed)

11anacaxbe-mixed
802.11a/n/ac/ax/be (mixed)

Auto
Automatic. In the 5 GHz mode, automatic selection provides either **11anac-mixed**, **11an-mixed**, or **Normal**.

Default:

Auto

2.37.1.2.8 Subbands

In the 5 GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Band-1
Band-2
Band-3
Band-1+2
Band-1+3
Band-2+3
Band-1+2+3

Default:

Band-1+2+3

2.37.1.2.9 QoS

With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the AP both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.2.10 DTIM-Period

This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

0 … 255

Default:

0

2.37.1.2.11 Background-Scan

In order to identify other APs within local radio range, the device can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the AP's "normal" radio activity, it is called a "background scan".

If a value is entered here, the device searches the frequencies in the active band that are currently not in use in cycles within this interval in order to find available APs.

The background scan function is usually deployed for rogue AP detection for the device in AP mode. This scan interval should correspond to the time span within which rogue APs should be recognized, e.g. 1 hour.

Conversely, for the device in client mode, the background scan function is generally used for improved mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

0 … 4294967296

Default:

0

Special values:

0

When the background scan time is "0" the background scanning function is deactivated.

2.37.1.2.12 Antenna-Gain

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly.

The field "Antenna gain" is for the gain of the antenna minus the actual cable loss. This value for true antenna gain is dynamically used to calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.

In contrast to this, the entry in the field "Tx-Power-Reduction" causes a static reduction in the power by the value entered, and ignores the other parameters.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

- 128 … + 127

Special values:

127

The internal default value for the antenna gain is used.

Default:

0

2.37.1.2.13 Tx-Power-Reduction

In contrast to antenna gain, the entry in the field **Tx power reduction** causes a static reduction in the power by the value entered, and ignores the other parameters.

The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

0 … 255

Default:

0

2.37.1.2.16 Indoor-Only-Operation

You can specify whether indoor-operation only is to be allowed.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.2.17 Activate-VLAN-Module-of-managed-APs

Use this item to activate or deactivate the VLAN module in the managed APs. If VLAN is switched off, all VLAN settings in the logical network are ignored.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.2.18 Mgmt-VLAN-Mode

VLAN mode for the management network. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated untagged even if VLAN is activated.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

untagged

The AP's management packets are not marked with a VLAN ID.

tagged

The AP's management packets are marked with the VLAN ID that is configured in this radio profile as the management VLAN ID.

Default:

untagged

2.37.1.2.19 Mgmt-VLAN-ID

VLAN ID for the management network. The management VLAN ID is used for tagging the management network which is used for communications between the WLC and the APs. VLAN is only used if the VLAN module in the access point is enabled. The management network can be operated without tagging even if VLAN is enabled by selecting the corresponding setting for the management VLAN mode. The VLAN ID "1" is reserved internally for this.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

2 … 4094

Default:

2

2.37.1.2.20 Report-seen-clients

By default, the access point only reports associated clients to the WLC. If all other seen clients should be reported, i.e. unassociated clients as well, you can activate this switch. This will increase the traffic on the network. You should therefore activate this switch only temporarily or for test purposes.

If you have a large number of unknown clients (e.g., with a Public Spot or in areas with lots of traffic), you should not activate this switch, otherwise you will be flooded by inbound messages.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.2.21 Client-Steering

This entry determines whether the AP should activate the client and/or band steering.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Off

Disables Client and Band Steering.

AP-based-Band-Steering

The AP independently directs the WLAN client to a preferred frequency band.

On

Activates the client and band steering controlled by the WLAN controller.

Client-Management

The client steering is performed decentrally by the client management of the APs introduced with LCOS 10.20.

Default:

Client-Management

2.37.1.2.22 Preferred-Band

This entry determines the frequency band that the AP preferably should direct the WLAN client.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

5GHz
2.4GHz

Default:

5GHz

2.37.1.2.23 Proberequest-Ageout-Seconds

This entry determines the length of time in seconds that the AP should store a WLAN client's connection. When this time expires, the AP deletes the entry from the table.

This value should be set to a low value if you are using clients in the WLAN that frequently switch from dual-band to single-band mode.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Max. 10 characters from `[0-9]`

Default:

120

Special values:

0

The AP immediately considers seen probe requests as invalid.

2.37.1.2.24 Adaptive-RF-Optimization

This entry is used to enable or disable the adaptive RF optimization feature.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

No

The feature is disabled.

Yes

The feature is enabled.

2.37.1.2.26 Subbands-6GHz

In the 6 GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

Band-5

2.37.1.2.27 6GHz-Mode

Specify which radio standards the physical WLAN interface you configured supports against a WLAN client in the 6 GHz frequency band.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

11axbe-mixed

802.11ax/be

Auto

Automatic. Within the 6 GHz mode, the automatic leads to 802.11ax.

Default:

Auto

2.37.1.2.29 Channel-Profile

Select the name of a channel profile. See *2.37.1.30 Channel-Profiles* on page 1291.

The DEFAULT profile activates all allowed channels of the set country.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

2.37.1.3 Commonprofiles

Here you define entire WLAN profiles that summarize all of the WLAN settings which can be used on the managed APs. This includes for example up to 16 logical WLAN networks and a set of physical WLAN parameters.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.3.1 Name

Name of the profile under which the settings are saved.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.3.2 Networks

List of the logical WLAN networks that are assigned via this profile.

From this list, APs use only the first eight entries that are compatible with their own hardware. This means that eight WLAN networks for purely 2.4 GHz operations and eight for purely 5 GHz operations can be defined in a profile. Consequently, each AP—be it a model offering 2.4 GHz or 5 GHz support—can choose from a maximum of eight logical WLAN networks.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.3.3 AP-Parameters

A set of physical parameters that the AP WLAN modules are supposed to work with.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.3.4 Controllers

A list of WLCs that the APs should attempt to connect with. The AP starts searching for a WLC with a broadcast. Defining alternative WLCs is worthwhile when a broadcast cannot reach all WLCs (e.g.if the WLC is located in another network).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 159 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.3.6 IEEE802.11u-General

Use this parameter to specify the name of the venue profile entered under **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles** that is to apply for the WLAN profile (i.e. the local common profile).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.3.7 Configuration-Delay

This parameter specifies the delay time before an AP executes a configuration update immediately after being rolled out by the WLC.

The delay time is primarily relevant for APs which are integrated into your managed WLAN via a radio link (e.g. via AutoWDS). This reduces the probability of undelivered configuration updates leading only to a partial configuration of your network, so making the other APs unreachable. The higher you set the delay time, the more likely it is that all unassociated APs will receive the configuration update rolled out by the WLC.

A value of at least 1 second per (AutoWDS-) hop is recommended.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables the delayed configuration update.

Default:

0

2.37.1.3.8 LED-Profile

The device LED profile selected here applies to the WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

2.37.1.3.9 LBS-General-Profile

The LBS general profile selected here applies to the WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

2.37.1.3.10 Wireless-ePaper-Profile

Enter the Wireless ePaper profile that is configured on the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.3.11 Event-Timeout

This entry sets the timeout for connections in seconds.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 10 characters from `[0-9]`

Default:

500

2.37.1.3.12 NTP-Profile

The WLAN controller synchronizes the time with an access point when it accepts it. As a result, it is possible that an access point that has been managed for a long time without new time information may have greater deviations from the WLAN controller, possibly leading to certificate problems. By using a time server, this problem cannot occur.

From the list of NTP profiles under *2.37.1.28 NTP-Profiles* on page 1288, select the profile that should apply in the WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.3.13 Link-Aggregation-Profile

Select the link aggregation profile from the list under *2.37.1.29 Link-Aggregation-Profiles* on page 1289 that should apply in the WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

max. 31 characters `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.3.248 Wireless-IDS-Profile

Use this entry to specify a wireless IDS profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default:

empty

2.37.1.4 Accesspoints

Here you define the APs that are to be managed from this WLC. At the same time you assign the WLAN profile to the AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.4.1 MAC-Address

MAC address of the AP.

The value `FFFFFFFFFFFF` defines the default configuration.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 12 characters from `[A-Z][a-z][0-9]:`

Default:

empty

2.37.1.4.2 Name

Name of the AP in managed mode.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.3 Location

Location of the AP in managed mode.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.4 Profile

This entry sets the WLAN profile that is to be used by this AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.6 Control-Connection-Encryption

Encryption for the communication over the control channel. Without encryption the control data is exchanged as cleartext. In both cases authentication is by certificate.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

default
Makes use of the encryption method defined in the 'Options' area.

DTLS

No

Default:

default

2.37.1.4.7 WLAN-Module-1

Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

default
Makes use of the encryption method defined in the “Options” area.

2.4GHz

5GHz

6GHz

Off

Auto

Default:

default

2.37.1.4.8 WLAN-Module-2

Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

default
Makes use of the encryption method defined in the “Options” area.

2.4GHz
5GHz
6GHz
Off
Auto

Default:

default

2.37.1.4.9 Module-1-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

In the 2.4 GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.10 Module-2-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

In the 2.4 GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.11 Operating

Activates or deactivates this entry.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

No
Yes

Default:

Yes

2.37.1.4.12 IP-Address

Valid static IP address for the AP if DHCP cannot/should not be used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.4.13 Netmask

Valid static netmask if DHCP cannot/should not be used.

This setting is not configurable with LANconfig.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.4.14 Gateway

Valid static IP address of the gateway if DHCP cannot/should not be used.

This setting is not configurable with LANconfig.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.4.16 Antenna-Mask

APs with 802.11 support can use up to three antennas for transmitting and receiving data. Depending on the application the use of the antennas can be set.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

1+2+3

When using the device in AP mode to connect wireless LAN clients it is generally recommended to use all three antennas in parallel in order to achieve good network coverage.

1+3

Antenna ports 1 and 3 are used for 2 parallel data streams for example in point to point connections with an appropriate dual slant antenna. The third antenna port is deactivated.

1

For applications with only one antenna (for example an outdoor application with just one antenna) the antenna is connected to port 1 and ports 2 and 3 are deactivated.

Auto

Automatic antenna selection.

All available antennas are used.

Default:

Auto

2.37.1.4.17 AP-Intranet

This references a line in the AP intranet table.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.18 Manage-Firmware

This allows the automatic firmware upload to be disabled for this AP. This is also automatically disabled by the controller in the case of certain errors. The reason for automatic deactivation is displayed in the column "Manage firmware additional information".

This setting is not configurable with LANconfig.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

No
Yes

Default:

Yes

2.37.1.4.19 Manage-Firmware-Additional-Information

This allows the automatic firmware upload to be disabled for this AP. This is also automatically disabled by the controller in the case of certain errors. The reason for automatic deactivation is displayed in the column "Manage firmware additional information".

This setting is not configurable with LANconfig.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

None
Disabled_due_to_error_during_update
Disabled_by_manual_upload

Default:

None

2.37.1.4.20 Module-1-Ant-Gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please

ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example:

AirLancer	Antenna gain	Cable attenuation:	Value to be entered
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

The current transmission power is displayed by the device's web interface or by telnet under **StatusWLAN statisticsWLAN parametersTransmission power** or with LANconfig under **System informationWLAN cardTransmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.4.21 Module-2-Ant-Gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example:

AirLancer	Antenna gain	Cable attenuation:	Value to be entered
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

The current transmission power is displayed by the device's web interface or by telnet under **StatusWLAN statisticsWLAN parametersTransmission power** or with LANconfig under **System informationWLAN cardTransmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.4.22 Module-1-TX-Reduct.

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.4.22 Module-2-TX-Reduct.

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

The current transmission power is displayed by the device's web interface or by telnet under **StatusWLAN statisticsWLAN parametersTransmission power** or with LANconfig under **System informationWLAN cardTransmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.4.24 Groups

Using this parameter, you optionally assign the corresponding AP profile to one or more tag groups. If you edit an AP profile, this parameter may additionally contain those assignment groups assigned by the WLC to the corresponding AP during the IP-dependent auto-configuration. Detailed information is available in the Reference Manual.

The tag groups are independent of the assignment groups, the assignment of which is specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. Manually assigning an assignment group has no effect on the AP configuration. The only effects are on the filtering in the command `show capwap group` at the console

The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**. Multiple entries can be provided in a comma-separated list.

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **Tag-Groups**. Multiple entries can be provided in a comma-separated list.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.25 Module-2-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 2nd physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Auto

The AP automatically detects the maximum channel bandwidth.

20MHz
The AP uses channels bundled at 20 MHz.

40MHz
The AP uses channels bundled at 40MHz.

80MHz
The AP uses channels bundled at 80MHz.

80+80MHz
The AP uses two channels bundled at 80 MHz.

160MHz
The AP uses channels bundled at 160 MHz.

Default:

Auto

2.37.1.4.26 Module-1-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 1st physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Automatic
The AP automatically detects the maximum channel bandwidth.

20MHz
The AP uses channels bundled at 20 MHz.

40MHz
The AP uses channels bundled at 40MHz.

80MHz
The AP uses channels bundled at 80MHz.

80+80MHz
The AP uses two channels bundled at 80 MHz.

160MHz
The AP uses channels bundled at 160 MHz.

Default:

Automatic

2.37.1.4.27 Client-Steering-Profile

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.28 LBS-Device-Location-Profile

With this entry, you assign a profile created under **Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location** to the AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 32 characters from `[A-Z][0-9]{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.29 Wireless-ePaper-Channel

Select a channel for the Wireless ePaper module from the drop down menu.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:

Auto

2.37.1.4.30 iBeacon-Profiles

Enter the iBeacon profile that is configured on the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.4.31 iBeacon-Channel

Set the transmit channel for the iBeacon module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

2402MHz
2426MHz
2480MHz

Default:

2402MHz

2426MHz

2480MHz

2.37.2.4.32 Minor

Specify here the unique minor ID of the iBeacon module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

0

2.37.1.4.33 iBeacon-Transmit-Power

Set the transmission power of the iBeacon module here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Low
The module sends with minimum power.

Medium
The module sends with medium power.

High
The module sends with maximum power.

Default:

High

2.37.1.4.34 SNMP-Comment

Enter a comment about this SNMP entry.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.35 Module-1-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Standard

The antenna gain value preset in the access point is used.

User defined

The value for **Module-1-Ant-Gain** is used.

Default:

Standard

2.37.1.4.36 Module-2-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Standard

The antenna gain value preset in the access point is used.

User defined

The value for **Module-2-Ant-Gain** is used.

Default:

Standard

2.37.1.4.37 Module-1-Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

Console path:

Setup > **WLAN-Management** > **AP-configuration** > **Accesspoints**

Possible values:

0 … 20

2.37.1.4.38 Module-2-Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

Console path:

Setup > **WLAN-Management** > **AP-configuration** > **Accesspoints**

Possible values:

0 … 20

2.37.1.4.39 WLAN-Module-3

Frequency of the third WLAN module. This parameter can also be used to deactivate the WLAN module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

default
Makes use of the encryption method defined in the “Options” area.

2.4GHz
5GHz
6GHz
Off
Auto

Default:

default

2.37.1.4.40 Module-3-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 2nd physical WLAN interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Auto
The AP automatically detects the maximum channel bandwidth.

20MHz
The AP uses channels bundled at 20 MHz.

40MHz
The AP uses channels bundled at 40 MHz.

80MHz

The AP uses channels bundled at 80 MHz.

80+80MHz

The AP uses two channels bundled at 80 MHz.

160MHz

The AP uses channels bundled at 160 MHz.

320MHz

The AP uses channels bundled at 320 MHz.

Default:

Auto

2.37.1.4.41 Module-3-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.4.42 Module-3-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Standard

The antenna gain value preset in the access point is used.

user-defined

The value for **Module-3-Ant-Gain** is used.

Default:

Standard

2.37.1.4.43 Module-3-Ant-Gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example:

AirLancer	Antenna gain	Cable attenuation:	Value to be entered
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.4.44 Module-3-TX-Reduct

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4 GHz band or 6.5 dBm in the 5 GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4 GHz band and 11.5 dBi in the 5 GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

2.37.1.5 WLAN-Modul-1-Default

This setting allows you to configure the frequency band in which the AP operates the 1st physical WLAN interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Auto

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 2.4GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4 GHz band.

5GHz

The AP operates the physical WLAN interface in the 5 GHz band.

6GHz

The AP operates the physical WLAN interface in the 6 GHz band.

Off

The AP disables the physical WLAN interface.

Default:

Auto

2.37.1.6 WLAN-Modul-2-Default

This setting allows you to configure the frequency band in which the AP operates the 2nd physical WLAN interface.

If a managed AP only has one physical WLAN interface, the AP ignores the settings for the 2nd physical WLAN interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Auto

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 5GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4 GHz band.

5GHz

The AP operates the physical WLAN interface in the 5 GHz band.

6GHz

The AP operates the physical WLAN interface in the 6 GHz band.

Off

The AP disables the physical WLAN interface.

Default:

Auto

2.37.1.7 Control-Connection-Encryption-default

Encryption for the communication over the control channel. Without encryption the control data is exchanged as cleartext. In both cases authentication is by certificate.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

DTLS
No

Default:

DTLS

2.37.1.8 Country-default

The country in which the AP is to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Albania
Argentina
Australia
Austria
Bahrain
Bangladesh
Belarus
Bosnia-Herzegovina
Brazil
Brunei Dar es Salaam
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Croatia
Cyprus
Czech Republic
Denmark
Ecuador
Egalistan
Egypt
Estonia
Finland
France
Germany
Ghana
Greece
Guatemala
Honduras
Hong-Kong
Hungary
Iceland
India
Indonesia
Ireland
Israel
Italy
Japan
Jordan
South Korea
Latvia
Lebanon
Liechtenstein
Lithuania
Luxembourg
Macao
Macedonia
Malaysia
Malta
Mexico
Moldavia

Morocco
Netherlands
New Zealand
Nicaragua
Norway
Oman
Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Puerto Rico
Qatar
Romania
Russia
Saudi Arabia
Singapore
Slovakia
Slovenia
South Africa
Spain
Sweden
Switzerland
Taiwan
Tanzania
Thailand
Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
Great Britain
United States FCC
Uruguay
Venezuela

Default:

Germany

2.37.1.9 AP-Intranets

If necessary, define IP parameter profiles here for use in the AP table if certain APs have IP addresses that were not assigned by DHCP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.9.1 Name

Name of the intranet where APs are operated. This name is only used for internal administration of intra-networks.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.9.2 Parent-Name

A WLC is capable of managing a wide range of different APs at different locations. However, WLAN profiles include settings that are not equally suitable for every type of AP that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles, it is possible for the intranets to "inherit" selected properties from other entries.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.9.3 Local-Values

Specifies which intranet parameters are taken over during inheritance from the parent element. All non-inherited parameters can be set locally for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 2 characters from `[0-9]`

Default:

00

2.37.1.9.4 Domain-name

Domain name used by the access point when resolving WLC addresses.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.9.5 Netmask

Static netmask if DHCP cannot be /should not be used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.9.6 Gateway

Static IP address of the gateway if DHCP cannot be /should not be used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.9.7 Primary-DNS-Srv

Static IP address of the first DNS server if DHCP cannot be /should not be used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.9.8 Secondary-DNS-Srv

Static IP address of the second DNS server if DHCP cannot be /should not be used.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.37.1.9.9 IPv4-Config-Pool-Start

The start of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

0.0.0.0 … 255,255,255,255

Default:

empty

2.37.1.9.10 IPv4-Config-Pool-End

The end of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Possible values:

0.0.0.0 … 255,255,255,255

Default:

empty

2.37.1.10 Predef.-Intranets

This table lists the predefined AP intranets.

The settings for the predefined intranets are used exclusively for internal communications between the device and LANconfig. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.10.1 Name

This is the name of the predefined AP intranet.

The settings for the predefined intranets are used exclusively for internal communications between the device and LANconfig. Do not alter the pre-set values for these parameters. An irregular configuration may cause the devices to behave unexpectedly during operations.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Predef.-Intranets**

2.37.1.12 DSCP-for-Control-Packets

This item allows you to set the prioritization of control packets by DiffServ (Differentiated Services).

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Best-Effort
Assured-Forwarding-11
Assured-Forwarding-12
Assured-Forwarding-13
Assured-Forwarding-21
Assured-Forwarding-22
Assured-Forwarding-23
Assured-Forwarding-31
Assured-Forwarding-32
Assured-Forwarding-33
Assured-Forwarding-41
Assured-Forwarding-42
Assured-Forwarding-43
Expedited-Forwarding

Default:

Best-Effort

2.37.1.13 DSCP-for-Data-Packets

This item allows you to set the prioritization of data packets by DiffServ (Differentiated Services).

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Best-Effort
Assured-Forwarding-11
Assured-Forwarding-12
Assured-Forwarding-13
Assured-Forwarding-21
Assured-Forwarding-22
Assured-Forwarding-23
Assured-Forwarding-31
Assured-Forwarding-32
Assured-Forwarding-33
Assured-Forwarding-41
Assured-Forwarding-42
Assured-Forwarding-43
Expedited-Forwarding

Default:

Best-Effort

2.37.1.14 Multicast-Networks

This table contains the settings for the transmission of CAPWAP multicast packets over the bridge interfaces.

When a WLC receives a broadcast or multicast packet from a network belonging to a certain SSID, then it has to forward this packet to all APs that work with that SSID. The WLC has two ways to reach all of these APs:

- The WLC copies the packet and sends it as a unicast to the relevant APs. The replication of packets increases the CPU load on the controller and the necessary bandwidths, which negatively impacts performance especially of WAN connections.
- The WLC sends the packet as a multicast. In this case, a single packet only has to be transmitted. However, multicast packets sent from a controller only reach those APs in its own broadcast domain. APs at the other end of a routed WAN link cannot receive multicast packets from the controller.

The forwarding of multicast packets depends on the devices operated on the WAN route.

The WLC regularly sends keep-alive multicast packets to the multicast group. If an AP responds to these packets, the controller is able to reach this AP with multicast packets. For all other APs, the controller copies the multicast packets it receives and sends them as a unicast to the appropriate APs.

If the transmission of CAPWAP multicast packets has been activated and a valid multicast IP address with port has been defined for the bridge interface, the device forwards the incoming broadcast and multicast packets as a multicast to this address.

To ensure that the information about associated WLAN clients and their multicast group memberships is kept up to date even when they switch between APs, devices operating multicast simultaneously activate IGMP snooping for continuous updates to the information on multicast structure.

In applications featuring multiple WLCs, multicast packets can lead to loops. In order to avoid loops due to multicasts when using the bridge, the WLC applies the following measures:

- The WLC ignores CAPWAP multicast packets. When working with a WLC data tunnel, the controller sends these packets as unicast.
- The WLC does not forward packets that carry a CAPWAP multicast address as the recipient.
- The WLC automatically enables IGMP snooping on all managed APs if CAPWAP works with multicast.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.14.1 Bridge-Interface

This item allows you to select one of the specified bridge interfaces as the bridge interface for the multicast settings.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Multicast-Networks**

2.37.1.14.2 Active

This item allows you to select one of the specified bridge interfaces as the bridge interface for the multicast settings.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Multicast-Networks**

Possible values:

No
Yes

Default:

No

2.37.1.14.3 Multicast-Address

Use this item to select an IP address to which the device sends CAPWAP multicast packets for the selected bridge interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Multicast-Networks**

Possible values:

Max. 15 characters from `[0-9].`

Default:

233.252.124.1 to 233.252.124.32 (IP addresses from the unassigned range)

2.37.1.14.4 Multicast-Port

This item allows you to select a port for transmitting CAPWAP multicast packets over the selected bridge interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Multicast-Networks**

Possible values:

Max. 5 characters from `[0-9]`

Default:

20000 … 20031

2.37.1.14.5 Loopback-Addr.

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

If the list of IP networks or loopback addresses contains an entry named "DMZ", the associated IP address will be used. Name of a loopback address.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Multicast-Networks**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LBO…LBF for the 16 loopback addresses.
Any valid IP address.

2.37.1.15 AutoWDS-Profiles

This table contains the parameters for the AutoWDS profiles which you assign to the individual APs by means of the WLAN profile in order to implement meshed networks. AutoWDS profiles collect the settings and limits that form the P2P topology and the AutoWDS base networks.

In simple network environments, the use of the preset AutoWDS profile "DEFAULT" is sufficient. If you use several different AutoWDS profiles, the following conditions should be observed:

- APs with different AutoWDS profiles cannot be connected to one other, neither automatically nor manually.
- The maximum number of AutoWDS profiles corresponds to the maximum possible number of WLAN profiles on the WLC.
- The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.
- If two different AutoWDS profiles are used, then the rollout SSIDs must also be different. Similarly, the linking of an AutoWDS profile to a WLAN profile must be unique and unequivocal. If this is not the case, the WLC reports a profile error.
- Each AutoWDS profile uses its own SSID. This reduces the number of SSIDs that are available for the profiles. If an SSID is used multiple times, the WLC reports a profile error.
- There is only one WLC-TUNNEL-AUTOWDS interface on the WLC. The individual rollout SSIDs therefore use the same interface on the WLC as the endpoint. By default, communication between the WLAN clients is disabled during the integration.
- When express integration is enabled, the rollout SSID for unconfigured WLAN clients is initially unimportant. This means that during an express integration, an AP is able to retrieve its configuration from the WLC via an AP with a different AutoWDS profile; however, in this case it only receives its AutoWDS profile and the manually configured topology entries and/or P2P links. The automatic generation of a P2P configuration does not take place if the AutoWDS

profiles of the two APs do not match. If only one AutoWDS profile is transferred in this case, the AP falls back to scan mode after the usual time: however, it has by then been assigned its AutoWDS rollout SSID and it then integrates with the corresponding AutoWDS APs (according to its profile).

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.15.0 Link-Calibration

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Deactivated
Capacity
Robustness

2.37.1.15.1 Name

Name of the AutoWDS profile which you reference from other tables.

The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Max. 15 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.15.2 Commonprofile

Enter the name of the WLAN profile which the AutoWDS base network is assigned to. All APs operating with this WLAN profile simultaneously deploy the corresponding AutoWDS base network.

Different AutoWDS profiles may not refer to the same WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.15.3 SSID

Enter the name of the logical WLAN network (SSID) that a managed AP uses to deploy the AutoWDS base network. In client mode, unassociated APs use the SSID entered here to receive a configuration from the WLC.

This SSID is reserved exclusively for this AutoWDS profile. The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within your WLAN infrastructure.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

AutoWDS-Rollout

2.37.1.15.4 Key

Enter the WPA2 passphrase for the AutoWDS base network supported by a managed AP. Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

min. 8 characters; max. 63 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.15.6 Operating

Specify whether the AutoWDS is enabled or disabled for the selected profile. Inactive profiles are not transmitted by the WLC to an AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

No
Yes

Default:

No

2.37.1.15.7 Allow-Express-Integration

Here you specify whether the APs of the corresponding WLAN profile permit the express integration of unassociated APs via the AutoWDS base network. If you enable this setting, the affected master APs send an additional vendor-specific identifier in their beacons (assuming you have enabled 'SSID broadcast' in the AutoWDS profile) and probe responses to signal the availability of this integration option to unassociated APs.

If you enable AutoWDS and prohibit express integration, the AutoWDS base network allows only the preconfigured integration of unassociated or already associated APs in client mode.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

No

The AutoWDS base network allows only the preconfigured integration for unassociated clients.

Yes

The AutoWDS base network allows preconfigured integration as well as express integration of unassociated APs.

Default:

No

2.37.1.15.8 Topology-Management

Enter which type of topology management the WLC uses for the respective AutoWDS profile.

Due to the assignment of the WLAN profile by the WLC, the slave APs simultaneously receive information about the topology of the meshed network The topology results directly from the hierarchy of the P2P connections established between the APs. The two affected WLAN interfaces form a P2P pairing for this: The physical WLAN interface of the unassociated AP becomes the P2P slave; that of the selected anchor AP becomes the P2P master.

Normally, the WLC handles the automatic calculation of the topology, where a slave AP generally connects with the closest master AP. Calculated in real-time, the topology is recorded by the WLC in the status table **AutoWDS-Auto-Topology** (SNMP-ID 1.73.2.13). If you use semi-automatic or manual management, you define the static P2P links in the setup table **AutoWDS-Topology**. To achieve this, you specify the relationships between the individual master APs and slave APs in a similar manner to a normal P2P connection.

The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.

For manual topology configuration, it is important for a configured P2P master AP within the topology to be closer to the WLC than a corresponding P2P slave AP. This is because a brief interruption to the P2P connection will cause the slave AP to scan for the master AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Automatic

The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.

Semi automatic

The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.

Manual

The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Default:

Automatic

2.37.1.15.10 Slave-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from slave AP to master AP. The setting only affects P2P connections which the WLC has generated automatically.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

2.37.1.15.11 Master-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from master AP to slave AP. The setting only affects P2P connections which the WLC has generated automatically.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

2.37.1.15.12 Link-Loss-Timeout

Specify the time after which the AP tags the connection to its P2P partner as interrupted. The setting only affects P2P connections which the WLC has generated automatically. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

The link-loss timeout is independent of the other timeouts. In the interests of stable connectivity of the overall AutoWDS base network, we recommend that you do not use a value less than the default value.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 4294967295 Seconds

Default:

4

2.37.1.15.14 Continuation

Specify the continuation time of the automatically generated P2P configuration.

The continuation time mentioned above refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is set to `0`, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *2.37.1.15.15 Time-till-Preconf-Scan* on page 1232 until the start of the automatic (re-)configuration for the preconfigured integration.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 9999 Minutes

Special values:

0

The AP immediately switches off its physical WLAN interface(s) as soon as contact to the WLC is lost. The device immediately deletes its configuration parameters so that the WLC must re-transmit them when reestablishing the connecting.

Select this setting to protect the configuration parameters that are relevant for security from unauthorized access and misuse (e.g., in case the AP is stolen).

9999

The configuration parameters are permanently stored in the device. The AP continues to operate regardless how long the contact to the WLC is lost.

Default:

0

2.37.1.15.15 Time-till-Preconf-Scan

Specify the wait time after which the AP switches to client mode and scans for an AutoWDS base network using the values in the preconfiguration (the SSID and passphrase that are stored in the AutoWDS profile), if all continuation times have expired. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase in order to subsequently perform the reconfiguration process.

Parallel to this process, the configured *wait time for the start of express integration*.

The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to `0`.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables preconfigured integration on the respective AP.

Default:

60

2.37.1.15.16 Time-till-Express-Scan

Specify the wait time after which the AP switches to client mode and scans for any AutoWDS base networks, if all continuation times and also the *wait time for the start of the preconfigured integration* have expired (if set). If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables express integration on the corresponding AP.

Default:

0

2.37.1.15.17 Interface-Pairing

Specify which type of interface pairings an anchor AP allows based on the AutoWDS profile assigned to it. The setting is mainly relevant for devices with more than a physical WLAN interface.

The interface pairing influences the search by the AP for suitable anchor APs in client mode, taking the participating WLAN interfaces into account. This specifies whether the unassociated AP has to connect to the equivalent physical WLAN interface of the anchor AP to integrate, or whether it may pair with other physical interfaces. The definition of the interface pairing makes it possible to exclude invalid pairings, which may occur due to the assignment of different frequency bands due to the WLC configuration.

For instance, the anchor APs of your AutoWDS base network might be operating with the physical WLAN interfaces WLAN-1 set to the 2.4GHz band and WLAN-2 on the 5GHz band: If, for example, an unassociated AP is using a physical WLAN interface to search on both frequency bands, the interface pairing **Strict** prevents it from selecting WLAN-1 in the 5 GHz band in order to connect with the WLAN-2 of the anchor AP. Although this connection would be legitimate for the WLC configuration, the different radio settings would make it impossible to establish the P2P connection. The unassociated AP would lose the connection and would have to start a reconfiguration process.

If, on the other hand, both physical WLAN interfaces transmit on the same band, the interface pairing **Mixed** is also permissible, as the problematic configuration described above cannot occur.

If possible, ensure that all APs on each physical WLAN interface consistently use the same frequency band (2.4 GHz or 5 GHz) to exclude any potential problems with the automatic topology configuration.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Automatic

The WLC checks if a problematic configuration can occur. If no problematic configuration occurs, it accepts the interface pairing via the anchor AP. Otherwise, the WLC rejects it and the unassociated AP must connect again.

Strict

An unassociated AP may only connect its physical WLAN interface X to the equivalent WLAN interface of the anchor AP.

Mixed

An unassociated AP may connect its physical WLAN interface X to any WLAN interface of the anchor AP.

Default:

Automatic

2.37.1.15.18 Slave-Radio-Multi-Hop

This parameter determines whether connection requests from unassociated APs can be accepted on the same physical WLAN interface that the anchor APs in your AutoWDS base network are using as slaves to connect to the master.

Disabling this parameter can improve the stability and the load distribution within your AutoWDS base network. As a result of this however, single-radio APs can no longer function as anchor APs for extending your AutoWDS base network, and are the end of a hierarchy branch.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

No

An anchor AP never accepts connection requests from unassociated APs on the same physical WLAN interface that it is using to connect to the AutoWDS base network as a slave. WLAN multi-hops are only possible on devices with two managed physical WLAN interfaces.

Yes

An anchor AP also accepts connection requests from unassociated APs on the same physical WLAN interface that it is using to connect to the AutoWDS base network as a slave. WLAN multi-hops are possible on devices with one or two managed physical WLAN interfaces.

Single-Radio-AP-Only

Case-specific setting:

The setting **Yes** applies to devices with one physical WLAN interface.

The setting **No** applies to devices with more than one physical WLAN interface.

Default:

No

2.37.1.15.19 Band

Specify the frequency band used by the APs for the AutoWDS base network.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

2.4GHz/5GHz

Both the 2.4 GHz and the 5 GHz bands are used for AutoWDS base network.

2.4GHz

Only the 2.4 GHz band is used for the AutoWDS base network.

5GHz

Only the 5 GHz band is used for the AutoWDS base network.

Default:

5GHz

2.37.1.15.20 Band

This parameter specifies whether or not the APs broadcast the SSID of the AutoWDS base network in their beacons.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Yes

The APs broadcast the SSID of the AutoWDS base network. The network is visible for other WLAN clients.

No

The APs hide the SSID of the AutoWDS base network. The network is invisible for other WLAN clients.

Default:

No

2.37.1.16 AutoWDS-Topology

In this table you specify the manual elements of the AutoWDS topology; or, more specifically, the P2P routes between the individual slave APs and master APs. The device only processes this table if you activated manual or semi-automatic *topology management*.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.16.0 Link-Calibration

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Default
Deactivated
Capacity
Robustness

2.37.1.16.1 AutoWDS-Profile

Name of the AutoWDS profile for which this manual P2P configuration applies.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Max. 15 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.16.2 Priority

Specify the priority of a P2P connection from the perspective of a slave AP's physical WLAN interface.

This setting is currently a placeholder as the evaluation of the priorities has not been implemented yet. Please always enter the value `0` for the priority.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

0 … 4294967295

Default:

empty

2.37.1.16.3 Slave-AP-Name

Enter the name of the AP which takes on the role of the slave.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profile**.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.16.4 Slave-AP-WLAN-Ifc.

Here you set the physical WLAN interface used by the slave AP for the P2P link to the master AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Selection from the available physical WLAN interfaces.

Default:

WLAN-1

2.37.1.16.6 Master-AP-Name

Enter the name of the AP which takes on the role of the master.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profile**.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.16.7 Master-AP-WLAN-Ifc.

Here you set the physical WLAN interface used by the master AP for the P2P link to the slave AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Selection from the available physical WLAN interfaces.

Default:

WLAN-1

2.37.1.16.9 Key

You can also enter an individual WPA2 passphrase for the P2P connection. If you leave the field empty, the device automatically generates a passphrase with a length of 32 characters.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

min. 8 characters; max. 63 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.16.10 Operating

Specify whether the P2P configuration is enabled or disabled for the selected Auto-WDS profile.

The WLC does not transmit disabled P2P configurations to the AP and, when evaluating the manual AutoWDS topology table in semi-automatic mode, it ignores disabled entries.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

No
Yes

Default:

No

2.37.1.16.12 Slave-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from slave AP to master AP. This setting only affects P2P connections that you created manually.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

2.37.1.16.13 Master-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from master AP to slave AP. This setting only affects P2P connections that you created manually.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

0 … 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

2.37.1.16.14 Link-Loss-Timeout

Specify the time after which the AP tags the connection to its P2P partner as interrupted. This setting only affects P2P connections that you created manually. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

The link-loss timeout is independent of the other timeouts. In the interests of stable connectivity of the overall AutoWDS base network, we recommend that you set the timeout to 4 seconds as a minimum.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

0 … 4294967295 Seconds

Special values:

0

For this value, the WLC retrieves the specified value for **Link-Loss-Timeout** from **Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profile**.

Default:

0

2.37.1.16.16 Continuation

Specify the continuation time of the manual P2P configuration.

The continuation time mentioned above refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is set to `0`, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

0 … 9999 Minutes

Special values:

0

The AP immediately switches off its physical WLAN interface(s) as soon as contact to the WLC is lost. The device immediately deletes its configuration parameters so that the WLC must re-transmit them when reestablishing the connecting.

Select this setting to protect the configuration parameters that are relevant for security from unauthorized access and misuse (e.g., in case the AP is stolen).

9999

The configuration parameters are permanently stored in the device. The AP continues to operate regardless how long the contact to the WLC is lost.

Default:

0

2.37.1.17 IEEE802.11u

The tables and parameters in this menu are used to make all settings for connections according to IEEE 802.11u and Hotspot 2.0. Profiles are used to assign these settings to the APs that are connected to the WLC.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.17.1 Network-Profiles

The table **Network profiles** is the highest administrative level for 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each of your created profiles, assigning downstream profile lists (such as those for ANQP or HS20) to them, or modifying general settings.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.1.1 Name

Use this parameter to give the 002.11u profile a name. You then assign a logical WLAN network to this profile in the table **Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles** under **802.11u-Profile**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.1.2 Operating

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.17.1.3 Hotspot2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.

The prerequisite for this function is that support for connections according to IEEE 802.11u is enabled.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.17.1.4 Internet

Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.17.1.5 Network-Type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Private

Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.

Private-GuestAcc

Similar to `Private`, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

Public-Charge

Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.

Public-Free

Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.

Personal-Dev

In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.

Emergency

Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

Experimental

Describes networks that are set up for testing purposes or are still in the setup stage.

Wildcard

Placeholder for previously undefined network types.

Default:

Private

2.37.1.17.1.6 Asra

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

No
Yes

Default:

No

2.37.1.17.1.7 HESSID-Type

Specify the HESSID to be transmitted by the device to the APs for the homogeneous ESS.

A homogeneous ESS is defined as a group of a specific number of APs, which all belong to the same network. The MAC address of a connected AP (its BSSID) or the MAC address of the WLC serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT".

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Auto
The device uses its own MAC address to generate a common HESSID for all of the APs with the relevant network profile.

user
Set an HESSID for all APs with the relevant network profile manually.

None
The connected APs are not assigned an HESSID.

Default:

Auto

2.37.1.17.1.8 HESSID-MAC

If you selected the setting `user` for the **HESSID-Type**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Set the HESSID to be either the BSSID of any AP in your homogeneous ESS or the MAC address of the WLC; enter it with capital letters and without separators, e.g., `008041AEFD7E` for the MAC address 00:80:41:ae:fd:7e.

If your AP is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Max. 12 characters from `[A-Z][a-z][0-9]`

Default:

000000000000

2.37.1.17.1.10 ANQP-Profile

Use this parameter to specify a valid ANQP profile from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles** that you want to use for the 802.11u profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.1.12 HS20-Profile

Use this parameter to specify a valid Hotspot-2.0 or HS20 profile profile from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot-2.0-Profiles** that you want to use for the 802.11u profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.2 ANQP-Profiles

Using this table you manage the profile lists for IEEE802.11u or ANQP. IEEE802.11u profiles offer you the ability to group certain ANQP elements and to assign them to mutually independent logical WLAN interfaces in the table **Network-Profiles**. These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.2.1 Name

Assign a name for the ANQP 2.0 profile here. You specify this name later in the table **Network-Profiles** under **ANQP profile**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.2.2 Include-in-Beacon-OUI

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional-OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9].,`

Default:

empty

2.37.1.17.2.3 Additional-OUI

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9].,`

Default:

empty

2.37.1.17.2.4 Domain-List

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from its home provider in order to avoid possible roaming costs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9].,`

Default:

empty

2.37.1.17.2.5 NAI-Realm-List

In this field, enter a valid NAI realm profile from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.2.6 Cellular-List

In this field, enter the name of a valid NAI realm profile from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.2.7 Network-Auth-Type-List

In this field, enter the name of one or more valid authentication parameters from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Auth-Type-List**.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.3 Hotspot2.0-Profiles

Using this table you manage the profile lists for the Hotspot 2.0. Hotspot -2.0 profiles offer you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to assign them to mutually independent logical WLAN interfaces in the table **Network-Profiles** under **HS20-Profile**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.3.1 Name

Assign a name for the Hotspot 2.0 profile here. You specify this name later in the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Profiles** under **HS20-Profile**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.3.2 Operator-Name

In this field, enter a valid profile for the hotspot operator from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.3.3 Connection-Capabilities

In this field, enter one or more valid entries for the connection capabilities from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Connection-Capability**. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown".

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.3.4 Operating-lass

Enter the code for the global operating class of the managed APs. The operating class is used to inform a station about the frequency bands and channels used by an AP. Example:

81

Operation at 2.4 GHz with channels 1-13.

116

Operation at 40 MHz with channels 36 and 44.

Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to an AP: Global operating classes, available at *standards.ieee.org*.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.3.5 Hotspot2.0-Release

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Release-1
Release-2

2.37.1.17.3.6 Domain-Id

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16-bit value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.37.1.17.3.7 OSU-Network-Name

Name of the SSID that provides access to the OSU server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.3.8 OSU-Providers

List of OSU provider names in *2.37.1.17.12 OSU-Providers* on page 1264 that are supported in the profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.4 Network-Authentication-Type

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

You specify the name of the network authentication type profile later in the table **ANQP-profiles** under **Network-Auth-Type-List**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.4.1 Name

Assign a name for the table entry, e.g., `Accept Terms and Conditions`.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.4.2 Network-Auth-Type

Choose the context from the list, which applies before forwarding.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Accept-Terms-Cond

An additional authentication step is set up that requires the user to accept the terms of use.

Online-Enrollment

An additional authentication step is set up that requires the user to register online first.

Http-Redirection

An additional authentication step is set up to which the user is forwarded via HTTP.

DNS-Redirection

An additional authentication step is set up to which the user is forwarded via DNS.

Default:

Accept-Terms-Cond

2.37.1.17.4.3 Redirect-URL

Enter the address to which the device forwards stations for additional authentication.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.5 Cellular-Network-Information-List

Using this table, you manage the profile lists for the cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.

In the setup menu you assign an ANQP profile to this list by using the table **ANQP-Profiles**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.5.1 Name

Assign a name for the cellular network profile, such as an abbreviation of the network operator in combination with the cellular network standard used. You specify this name later in the table **ANQP-Profiles** under **Cellular-List**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.5.2 Country-Code

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.37.1.17.5.3 Network-Code

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.37.1.17.6 Venue-Name

In this table, enter general information about the location of an AP.

In the event of a manual search, additional details on the Venue information help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.6.1 Name

Enter a name for the list entry in the table. This name will be used to reference the site information from other tables.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.6.2 Language

Select the language in which you store information about the location.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian

Default:

None

2.37.1.17.6.3 Venue-Name

Enter a short description of the location of your device for the selected language.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.7 NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.

In the setup menu you assign an ANQP profile to this list by using the table **ANQP-Profiles**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.7.1 Name

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. You specify this name later in the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Profiles** under **HS20-Profile**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.7.2 NAI realm

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest case, is `<username>@<realm>`, for `user746@providerX.org`, and therefore the corresponding realm is `providerX.org`.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.17.7.3 EAP method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication procedure

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

Possible values:

None

Select this setting when the relevant NAI realm does not require authentication.

EAP-TLS

Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate installed by the user.

EAP-SIM

Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.

EAP-TTLS

Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.

EAP-AKA

Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

Default:

None

2.37.1.17.7.4 Auth-Parameter-List

In this field, enter the appropriate authentication parameters for the EAP method using a comma-separated list, e.g., for EAP-TTLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` or for EAP-TLS `Credentials.Certificate`.

Also, specify one of the names from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Auth-Parameter**.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.8 Operator list

Using this table you manage the cleartext name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.8.1 Name

Assign a name for the entry, such as an index number or combination of operator-name and language.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.8.2 Language

Select a language for the hotspot operator from the list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian

Default:

None

2.37.1.17.8.3 Operator name

Enter the cleartext name of the hotspot operator.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.9 General

This table is used to manage the general settings for IEEE 802.11u/Hotspot 2.0.

On a standalone AP, these settings are available as separate parameters. On a WLC these parameter are collected into tables, which are ultimately assigned to the managed APs by means of the WLAN profile (table **Commonprofiles**).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.9.1 Name

Assign a name for the general-settings profile here. You specify this name later in the table **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles** under **Hotspot2.0-General**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.17.9.2 Link status

Using this entry, you specify the connectivity status of your device to the Internet.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Auto

The device determines the status value for this parameter automatically

Link-Up

The connection to the Internet is established.

Link-Down

The connection to the Internet is interrupted.

Link-Test

The connection to the Internet is being established or is being checked.

Default:

Auto

2.37.1.17.9.3 Downlink speed

Using this entry, you enter the nominal value for the maximum receiving bandwidth (downlink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

0 … 4294967295 Kbps

Default:

0

2.37.1.17.9.4 Uplink-Speed

Using this entry you can enter the nominal value for the maximum transmission bandwidth (uplink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

0 … 4294967295 Kbps

Default:

0

2.37.1.17.9.5 IPv4-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv4.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Not-Available
IPv4 address type is not available.

Public-Addr-Available
Public IPv4 address is available.

Port-Restr-Addr-Avail
Port-restricted IPv4 address is available.

Single-Nat-Priv-Addr-Avail
Private, single NAT-masked IPv4 address is available.

Double-Nat-Priv-Addr-Avail
Private, double NAT-masked IPv4 address is available.

Port-Restr-Single-Nat-Addr-Avail
Port-restricted IPv4 address and single NAT-masked IPv4 address is available.

Port-Restr-Double-Nat-Addr-Avail
Port-restricted IPv4 address and double NAT-masked IPv4 address is available.

Availability-not-known
The availability of an IPv4 address type is unknown.

Default:

Single-Nat-Priv-Addr-Avail

2.37.1.17.9.6 IPv6-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv6.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Not-Available
IPv6 address type is not available.

Available
IPv6 address type is available.

Availability-not-known
The availability of an IPv6 address type is unknown.

Default:

Not-Available

2.37.1.17.9.7 Venue group

The venue group describes the environment where you set up the AP. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Unspecified
Unspecified

Assembly
Assembly

Business
Business

Educational
Educational

Factory-and-Industrial
Factory and industry

Institutional
Institutional

Mercantile
Mercantile

Residential
Residential

Storage
Storage

Utility and miscellaneous
Utility and miscellaneous

Vehicular
Vehicular

Outdoor
Outdoor

Default:

Educational

2.37.1.17.9.8 Venue type

Using the location type code (venue type), you have the option to specify details for the location group. These values are also specified by the standard. The possible type codes can be found in the following table.

Defining venue groups

Table 14: Overview of possible values for venue groups and types

Venue group	Code = Venue-Type-Code
Unspecified	
Assembly	> 0 = unspecified assembly > 1 = stage > 2 = stadium

Venue group	Code = Venue-Type-Code
	> 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) > 4 = amphitheater > 5 = amusement park > 6 = place of worship > 7 = convention center > 8 = library > 9 = museum > 10 = restaurant > 11 = theater > 12 = bar > 13 = café > 14 = zoo, aquarium > 15 = emergency control center
Business	> 0 = unspecified business > 1 = doctor's office > 2 = bank > 3 = fire station > 4 = police station > 6 = post office > 7 = office > 8 = research facility > 9 = law firm
Educational:	> 0 = unspecified education > 1 = primary school > 2 = secondary school > 3 = college
Factory and industry	> 0 = unspecified factory and industry > 1 = factory
Institutional	> 0 = unspecified institution > 1 = hospital > 2 = long-term care facility (e.g., nursing home, hospice) > 3 = rehabilitation clinic > 4 = organizational association > 5 = prison
Mercantile	> 0 = unspecified commerce > 1 = retail store > 2 = food store > 3 = Automobile workshop > 4 = shopping center > 5 = gas station
Halls of residence	> 0 = unspecified residence hall > 1 = private residence > 2 = hotel or motel > 3 = student housing

Venue group	Code = Venue-Type-Code
	› 4 = guesthouse
Warehouse	› 0 = unspecified warehouse
Utility and miscellaneous	› 0 = unspecified service and miscellaneous
Vehicular	› 0 = unspecified vehicle › 1 = passenger or transport vehicles › 2 = aircraft › 3 = bus › 4 = ferry › 5 = ship or boat › 6 = train › 7 = motorcycle
Outdoor	› 0 = unspecified outdoor › 1 = Municipal WLAN network › 2 = city park › 3 = rest area › 4 = traffic control › 5 = bus stop › 6 = kiosk

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

2.37.1.17.9.9 Venue name

Use this field to specify one or more valid list entries from the table **Venue Name** in order to identify the location of the device. The parameter considers all list entries that match the venue name specified here.

Multiple names can be provided in a hash-sign-separated ('#') list.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.17.10 Auth parameter

This table contains a set list of possible authentication parameters for the NAI realms. You reference this list in the table **NAI-Realms** as a comma-separated list in the input field **Auth-Parameter**.

Table 15: Overview of possible authentication parameters

Parameter	Sub-Parameter	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password
	None	No credentials required
TunnelEAPCredentials.*		
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.10.1 Name

This entry displays the name of the authentication parameters that you referenced as a comma-separated list in the table **NAI-Realms** in the input field **Auth-Parameter**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Auth-Parameter**

2.37.1.17.11 Connection capability

This table contains a set list of the connection capabilities that you referenced as a comma-separated list in the table **Hotspot2.0-Profiles** in the input field **Connection-Capabilities**. Possible status values for each of these services are 'closed' (**-C**), 'open' (**-O**) or 'unknown' (**-U**).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.11.1 Name

This entry displays the name of the connection capability that you referenced as a comma-separated list in the table **Hotspot2.0-Profiles** in the input field **Connection-Capabilities**.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Connection-Capability**

2.37.1.17.12 OSU-Providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

2.37.1.17.12.1 Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.37.1.17.12.2 Language

Set the language supported by this OSU provider.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian
Korean

2.37.1.17.12.3 Friendly-Name

Give this OSU provider a descriptive name.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.1.17.12.4 OSU-Methods

Set the OSU methods used by this OSU provider. See also *2.71.7.11 OSU-Methods* on page 1658. Options are "OMA-DM" or "SOAP-XML-SPP".

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.1.17.12.5 URI

Enter a URI where a client can reach the OSU server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.1.17.12.6 NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.1.17.12.7 Service-Description

Enter a descriptive text for this service here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.1.17.12.8 Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the **File management** feature. We recommend PNG as the file format.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

None
OSU-Prov-Img-1
OSU-Prov-Img-2
OSU-Prov-Img-3
OSU-Prov-Img-4
OSU-Prov-Img-5
OSU-Prov-Img-6
OSU-Prov-Img-7
OSU-Prov-Img-8
OSU-Prov-Img-9
OSU-Prov-Img-10
OSU-Prov-Img-11
OSU-Prov-Img-12
OSU-Prov-Img-13
OSU-Prov-Img-14
OSU-Prov-Img-15
OSU-Prov-Img-16

2.37.1.17.12.9 Icon-Language

This item sets the language for the selected icon.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **OSU-Providers**

Possible values:

None
English
German
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabic
Korean

2.37.1.18 Config-Assignment-Groups

This table contains the assignment groups. Based on these, the WLC automatically assigns the network configuration, a WLAN profile and a client-steering profile to the unassociated APs. For this purpose, you specify an IP address range for each individual assignment group. For example, in a centrally managed WLAN you can use IP address ranges to automatically assign a location-specific configuration to unassociated APs (e.g., Branch A, Branch B, etc.).

An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups should overlap, LCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status** > **WLAN-Management** > **AP-Configuration**.

Please ensure that the AP table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.18.1 Name

Name of the assignment group which you reference from other tables.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.18.2 Profile

Name of the WLAN profile that the WLC automatically assigns to an unassociated AP via the assignment group.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.18.3 AP-Intranet

Name of the IP parameter profile that the WLC automatically assigns to an unassociated AP via the assignment group.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **AP-Intranets**

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Special values:

DHCP

The AP retrieves its network configuration via DHCP.

Default:

empty

2.37.1.18.4 IPv4-Reference-Pool-Start

Start of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

0.0.0.0 … 255,255,255,255

Default:

empty

2.37.1.18.5 IPv4-Reference-Pool-End

End of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

0.0.0.0 … 255,255,255,255

Default:

empty

2.37.1.18.6 Client steering profile

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

Name from **Setup** > **WLAN-Management** > **Client-Steering** > **Profiles**

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.18.7 iBeacon-Profiles

Enter the iBeacon profile that is configured on the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Config-Assignment-Groups**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.37.1.20 Tag groups

This table contains the tag groups that the WLC automatically assigns to the APs belonging to a WLAN profile. Among other things, tag groups allow actions performed on the WLC to be restricted to a selection of APs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.20.1 Name

You use this parameter to specify the name of the tag being created.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Tag-Groups**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'() +-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.21 LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile and assign this to a WLAN profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.21.1 Name

Give a name to the device LED profile here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

2.37.1.21.4 LED mode

Set the operating mode for the LEDs here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

On

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

Default:

On

2.37.1.21.5 LED off seconds

In the operating mode **Timed off** you can specify the delay in seconds after which the LEDs are disabled following a restart. This is useful for the LEDs to indicate critical errors during the restart process.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

Max. 4 characters from `[0-9]`

Default:

300

2.37.1.22 LBS

This is where you configure the settings for the LANCOM location-based services (LBS).

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.22.1 General

In this directory you configure the general settings for the LANCOM location-based services (LBS).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS**

2.37.1.22.1.0 Use TLS connection

This entry is used to enable or disable the use of TLS connections.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

No
Yes

Default:

No

2.37.1.22.1.1 Name

Enter a description of the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Max. 251 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.22.1.2 Operating

Enables or disables the location-based services.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

No

2.37.1.22.1.4 LBS server address

Enter the address of the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.22.1.5 LBS server port

Enter the port used by the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Max. 4 characters from `[0-9]`

Default:

9090

2.37.1.22.1.6 User name

This entry contains the user name used by the device to login to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.22.1.7 Password

This entry contains the password used by the device to authenticate at the LBS server.

Repeat the password in the next field.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.22.1.8 Aggregation

Use this entry to determine whether larger amounts of data are to be aggregated.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

No

2.37.1.22.1.9 Sequence-Number-Transmit

This entry specifies whether the device sends its sequence number to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.10 SSID-Transmit

Determines whether the device transmits its SSID to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.11 Interface-Identifier-Transmit

This entry specifies whether the device sends the name of the interface used to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.12 BSSID-Transmit

This entry determines whether the Basic Service Set Identification (BSSID) of the device is transmitted to the LBS server. Typically, the BSSID is the MAC address of the AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.13 Signal-Level-Transmit

This entry determines whether the signal strength used by the device is transmitted to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.14 Frequency-Transmit

This entry determines whether the frequency used by the device is transmitted to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.15 Noise-Transmit

This entry specifies whether the device sends the noise value to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.1.16 WLAN-Frame-Type-Transmit

This entry determines whether the device transmits the WLAN-Frame-Type to the LBS server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

Possible values:

Yes
No

Default:

Yes

2.37.1.22.2 Device location

This table is used to set the coordinates of the device location. The position is defined in geographical coordinates (degrees, minutes, seconds, orientation).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS**

2.37.1.22.2.1 Name

Enter a description of the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 251 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.22.2.2 Floor

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

0

2.37.1.22.2.3 Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

0

2.37.1.22.2.12 Description

Enter a description of the device.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 251 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.22.2.13 Latitude-Decimal-Degree

Enter the latitude of the location of the device in decimal degrees.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 12 characters from `[0-9].`

Default:

empty

2.37.1.22.2.14 Longitude-Decimal-Degree

Enter the longitude of the location of the device in decimal degrees.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

Possible values:

Max. 12 characters from `[0-9].`

Default:

empty

2.37.1.23 Wireless ePaper profile

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.23.1 Name

Specify the name of the Wireless ePaper profile here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

DEFAULT

2.37.1.23.2 Operating

Specify whether the selected Wireless ePaper profile is enabled or disabled. Inactive profiles are not transmitted by the WLC to an AP.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

Possible values:

No

The selected Wireless ePaper profile is not enabled.

Yes

The selected Wireless ePaper profile is enabled.

Default:

Yes

2.37.1.23.3 Port

Enter the port used for the Wireless ePaper module.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

7353

2.37.1.23.4 Outbound-Server

IP address of the Wireless ePaper Server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9].-:%`

2.37.1.23.5 Loopback-Address

Enter loopback address here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.24 iBeacon-Profiles

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.24.1 Name

Specify the name of the iBeacon profile that should be supplied to the APs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **iBeacon-Profile**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.24.2 Operating

Specify whether the selected iBeacon profile is enabled or disabled. Inactive profiles are not transmitted by the WLC to an AP

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **iBeacon-Profile**

Possible values:

No

The selected iBeacon profile is not enabled.

Yes

The selected iBeacon profile is enabled.

Default:

No

2.37.1.24.3 Major

Specify the unique major ID of the iBeacon profile that the WLC is to supply to the APs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **iBeacon-Profile**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.37.1.24.4 UUID

Specify the "universally unique identifier" (UUID) of the iBeacon module that should be transmitted to the APs.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **iBeacon-Profile**

Possible values:

Max. 36 characters from `[0-9][a-f][A-F]-`

Default:

00000000-0000-0000-0000-000000000000

2.37.1.25 LEPS-U

LANCOM Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.25.1 Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

2.37.1.25.1.1 Name

Enter a unique name for the LEPS-U profile here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.37.1.25.1.2 Network profile

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. 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-U profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.37.1.25.1.3 Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

2.37.1.25.1.4 Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

2.37.1.25.1.5 VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 4 characters from `[0-9]`

2.37.1.25.2 Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

2.37.1.25.2.1 Name

Enter a unique name for the LEPS-U user here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.37.1.25.2.2 Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.37.1.25.2.3 WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

2.37.1.25.2.4 Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

2.37.1.25.2.5 Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

2.37.1.25.2.6 VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0-9]`

2.37.1.26 Timeframe

Time frames are used when a WLAN SSID should not be broadcast permanently. One profile may contain several lines with different timeframes. Different lines in a timeframe should complement one another, i.e. if you specify WORKTIME you will should probably specify a timeframe called FREETIME to cover the time outside of working hours.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.26.1 Name

Enter the name of the timeframe for referencing.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Timeframe**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.26.2 Home

Here you set the start time (time of day) in the format HH:MM when the selected profile becomes valid.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Timeframe**

Possible values:

Max. 5 characters from `[0-9]:`

Default:

00:00

2.37.1.26.3 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 from HH:MM normally goes to HH:MM:00, with the exception of stop time 00:00, which is interpreted as 23:59:59.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Timeframe**

Possible values:

Max. 5 characters from `[0-9]:`

Default:

00:00

2.37.1.26.4 Weekdays

Here you select the weekday on which the timeframe is to be valid.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Timeframe**

Possible values:

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

Default:

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

2.37.1.27 Holidays

This table contains the holidays that have been defined.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.27.1 Index

This describes the position of the entry in the table.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Holidays**

Possible values:

0 … 9999

Default:

empty

2.37.1.27.2 Date

If you have created entries in the time control table that should apply on public holidays, enter the days here.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Holidays**

Possible values:

Max. 10 characters from `[0-9].`

Default:

empty

2.37.1.28 NTP-Profiles

In this table you can find the NTP profiles of the defined time servers.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.28.1 Name

The name of this NTP profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.28.2 RQ-Address

The server name or IP address of the NTP server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.28.3 Authentication-Enabled

Enables or disables MD5 authentication for the server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

No
Disabled
Yes
Enabled

Default:

No

2.37.1.28.4 Key-ID

Identifies the key used for MD5 authentication for the server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

1 … 65535

2.37.1.28.5 Key

The value of the key for authentication with the NTP server.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.1.29 Link-Aggregation-Profiles

LACP according to IEEE 802.1AX allows several Ethernet connections to be bundled in a so-called LAG (Link Aggregation Group) in order to increase the achievable data throughput within the LAG. For this purpose, the outgoing packets on the sending side are distributed to the various individual links within the LAG on the basis of the configured frame distribution policy.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.29.1 Name

The name of this LAG (Link Aggregation Group).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Link-Aggregation-Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.1.29.2 Operating

Enables or disables this LAG (Link Aggregation Group).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Link-Aggregation-Profiles**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

2.37.1.29.3 System-Priority

The system priority of this LAG (Link Aggregation Group).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Link-Aggregation-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

32768

2.37.1.29.4 Frame-Distribution-Policy

Frame distribution policy of this LAG (Link Aggregation Group).

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Link-Aggregation-Profiles**

Possible values:

Flow-Hash

For outgoing packets, a flow hash is formed over the IP addresses and TCP/UDP ports contained and the packets are distributed to the individual links of the LAG on the basis of this. This achieves a distribution at session level, so that sessions of a single client can also be distributed to multiple links. This setting is recommended for most scenarios.

Source-Dest-MAC

Outgoing packets are distributed to the individual links of the LAG based on the contained pair of source MAC address and destination MAC address.

Default:

Flow-Hash

2.37.1.30 Channel-Profiles

Use this table to create the configuration of the WLAN channels.Within the channel profile, the WLAN channels can be defined per frequency band. In this way, you can also uniquely define channels whose numbering is repeated in different frequency bands (e.g., at 2.4 GHz and 6 GHz). Then link newly created channel profiles within the physical WLAN profile.

The DEFAULT profile activates all allowed channels.

Pfad Konsole:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.30.1 Name

Name of the profile. Specify it in *2.37.1.2.29 Channel-Profile* on page 1193.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Channel-Profiles**

2.37.1.30.2 2.4GHz-Channels

Select the 2.4 GHz channels for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Channel-Profiles**

2.37.1.30.3 5GHz-Channels

Select the 5 GHz channels for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Channel-Profiles**

2.37.1.30.4 6GHz-Channels

Select the 6 GHz channels for this profile.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Channel-Profiles**

2.37.1.41 WLAN-Modul-3-default

This setting allows you to configure the frequency band in which the AP operates the 3rd physical WLAN interface.

If a managed AP only has two ot less physical WLAN interfaces, the AP ignores the settings for the 3rd physical WLAN interface.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Auto

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 6GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4Ghz band.

5GHz

The AP operates the physical WLAN interface in the 5Ghz band.

6GHz

The AP operates the physical WLAN interface in the 6Ghz band.

Off

The AP disables the physical WLAN interface.

Default:

Auto

2.37.1.249 Wireless-IDS

This menu contains the settings for Wireless-IDS.

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

2.37.1.249.1 Wireless-IDS

Here, you configure wireless IDS.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

2.37.1.249.1.1 Name

This entry contains the setup values for Name.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.2 Operating

This entry contains the setup values for Operating.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.3 EAPOLStartCounterLimit

This entry contains the setup values for EAPOLStartCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.4 EAPOLStartCounterInterval

This entry contains the setup values for EAPOLStartCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.5 ProbeBroadCounterLimit

This entry contains the setup values for ProbeBroadCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.6 ProbeBroadCounterInterval

This entry contains the setup values for ProbeBroadCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.7 DeauthenticateBroadCounterLimit

This entry contains the setup values for DeauthenticateBroadCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.8 DeauthenticateBroadCounterInterval

This entry contains the setup values for DeauthenticateBroadCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.9 DeauthenticateCounterLimit

This entry contains the setup values for DeauthenticateCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.10 DeauthenticateCounterInterval

This entry contains the setup values for DeauthenticateCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.11 AssociateReqCounterLimit

This entry contains the setup values for AssociateReqCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.12 AssociateReqCounterInterval

This entry contains the setup values for AssociateReqCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.13 ReAssociateReqCounterLimit

This entry contains the setup values for ReAssociateReqCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.14 ReAssociateReqCounterInterval

This entry contains the setup values for ReAssociateReqCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.15 AuthenticateCounterLimit

This entry contains the setup values for AuthenticateCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.16 AuthenticateCounterInterval

This entry contains the setup values for AuthenticateCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.17 DisAssociateCounterLimit

This entry contains the setup values for DisAssociateCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.18 DisAssociateCounterInterval

This entry contains the setup values for DisAssociateCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.19 IDS-Operational

This entry contains the setup values for IDS-Operational.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.20 Syslog-Operational

This entry contains the setup values for Syslog-Operational.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.21 SNMPTraps-Operational

This entry contains the setup values for SNMPTraps-Operational.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.22 E-mail

This entry contains the setup values for e-mail.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.23 E-mail recipient

This entry contains the setup values for the e-mail recipient.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.24 E-Mail-Aggregate-Interval

This entry contains the setup values for the E-Mail-Aggregate-Interval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.26 BlockAck-Out-Of-Window-Counter

This entry contains the setup values for BlockAck-Out-Of-Window-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.27 BlockAck-Out-Of-Window-Counter-Time

This entry contains the setup values for BlockAck-Out-Of-Window-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.28 BlockAck-Frames-Rx-After-D-E-L-B-A-Counter

This entry contains the setup values for BlockAck-Frames-Rx-After-D-E-L-B-A-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.29 BlockAck-Frames-Rx-After-D-E-L-B-A-Counter-Time

This entry contains the setup values for BlockAck-Frames-Rx-After-D-E-L-B-A-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.31 Null-Data-DoS-Counter

This entry contains the setup values for the Null-Data-DoS-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.32 Null-Data-DoS-Counter-Time

This entry contains the setup values for the Null-Data-DoS-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.34 Null-Data-P-S-Buffer-Overflow-Counter

This entry contains the setup values for the Null-Data-P-S-Buffer-Overflow-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.35 Null-Data-P-S-Buffer-Overflow-Counter-Time

This entry contains the setup values for the Null-Data-P-S-Buffer-Overflow-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.37 P-S-Poll-T-I-M-Interval-Diff

This entry contains the setup values for the P-S-Poll-T-I-M-Interval-Diff.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.38 P-S-Poll-T-I-M-Interval-Diff-Counter

This entry contains the setup values for the P-S-Poll-T-I-M-Interval-Diff-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.39 P-S-Poll-T-I-M-Interval-Diff-Counter-Time

This entry contains the setup values for the P-S-Poll-T-I-M-Interval-Diff-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.41 S-M-P-S-Mul-Stream-Frame-Counter

This entry contains the setup values for the S-M-P-S-Mul-Stream-Frame-Counter.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.42 S-M-P-S-Mul-Stream-Frame-Counter-Time

This entry contains the setup values for the S-M-P-S-Mul-Stream-Frame-Counter-Time.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.45 DisAssociateBroadCounterLimit

This entry contains the setup values for DisAssociateBroadCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.46 DisAssociateBroadCounterInterval

This entry contains the setup values for DisAssociateBroadCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.47 EAPOLSuccessCounterLimit

This entry contains the setup values for EAPOLSuccessCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.48 EAPOLSuccessCounterInterval

This entry contains the setup values for EAPOLSuccessCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.49 EAPOLFailureCounterLimit

This entry contains the setup values for EAPOLFailureCounterLimit.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.50 EAPOLFailureCounterInterval

This entry contains the setup values for EAPOLFailureCounterInterval.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.1.51 Promiscuous-Mode

This entry contains the setup values for Promiscuous-Mode.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **Wireless-IDS**

2.37.1.249.2 White list table

This menu contains the white list table.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

2.37.1.249.2.1 White-List-Id

This entry contains the setup values for White-List-Id.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **White-List-Table**

2.37.1.249.2.2 Station MAC

This entry contains the setup values for Station-MAC.

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS** > **White-List-Table**

2.37.5 CAPWAP-Port

Port number for the CAPWAP service.

This value is not configurable with LANconfig.

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 65535

Default:

1027

2.37.6 Autoaccept-AP

Enables the WLC to provide all new APs with a configuration, even those not in possession of a valid certificate.

Enables the WLC to provide a certificate to all new APs without a valid certificate. One of two conditions must be fulfilled for this:

- A configuration for the AP is entered into the AP table under its MAC address.

- The option "Automatically provide APs with the default configuration" is enabled.

Combining the settings for auto-accept and default configuration can cater for a variety of different situations for the setup and operation of APs:

Auto-Accept ON, Default-Configuration ON

Rollout phase: Use this combination only if you can be sure that no APs can connect unintentionally with the LAN and thus be accepted into the WLAN infrastructure.

Auto-Accept ON, Default-Configuration OFF

Controlled rollout phase: Use this combination if you have entered all of the approved APs into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.

Auto-Accept OFF, Default-Configuration OFF

Normal operation: No new APs will be accepted into the WLAN infrastructure without the administrator's approval.

Console path:

Setup > **WLAN-Management**

Possible values:

No
Yes

Default:

No

2.37.7 Accept-AP

This action triggers the integration of a new AP. The action accepts different arguments depending on the firmware version of the device. A MAC address must be specified in any case; further arguments are optional.

Syntax used in versions before LCOS 9.00

```
[-c] <WTP-MAC> [<Profile>] [<Name>] [<IP>] [<Netmask>] [<Gateway>]
```

Syntax used in versions as of LCOS 9.00

```
<WTP-MAC> [<WTP-MAC-2> … <WTP-MAC-n> ] [-c] [-l <Location>] [-p <Profile>] [-i <IP>] [-n <Name>] [-m
 <Netmask>] [-g <Gateway>] [-1 <Wlan1Channels>] [-2 <Wlan2Channels>]
```

If you define multiple MAC addresses, the device ignores the arguments `[-i <IP>]` and `[-n <Name>]`.

Console path:

Setup > **WLAN-Management**

Possible arguments:

-c

The WLC generates a configuration entry for the AP.

-l <Location>

The WLC supplements the AP configuration with the specified location.

We recommend that you store each location in the device as a unique field value pair so that, for example, the filter function in LCOS can be used at the console. The following field names are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

-p <Profile>

The WLC supplements the AP configuration with the specified WLAN profile.

-i <IP>

The WLC supplements the AP configuration with the specified IPv4 address.

-n <Name>

The WLC supplements the AP configuration with the specified device identifier.

-m <Netmask>

The WLC supplements the AP configuration with the specified netmask.

-g <Gateway>

The WLC supplements the AP configuration with the specified gateway address (IPv4).

-1 <Wlan1Channels>

The WLC supplements the AP configuration with the first channel list.

-2 <Wlan2Channels>

The WLC supplements the AP configuration with the second channel list.

2.37.8 Provide-default-configuration

This enables the WLC to assign a default configuration to every new AP (even those without a valid certificate), even if no explicit configuration has been stored for it. In combination with auto-accept, the WLC can accept all managed-mode APs which are found in the WLAN infrastructure managed by it (up to the maximum number of APs that can be managed by one WLC).

This option can also lead to the acceptance of unintended APs into the WLAN infrastructure. For this reason this option should only be activated during the start-up phase when setting up a centrally managed WLAN infrastructure.

Console path:

Setup > **WLAN-Management**

Possible values:

No
Yes

Default:

No

2.37.9 Disconnect AP

Do command to disconnect APs. The MAC address must be specified as a parameter.

Console path:

Setup > **WLAN-Management**

Possible values:

Syntax:

```
do Disconnect-AP <WTP-MAC>
```

2.37.10 News

This menu contains the configuration of the notification system of the WLAN management.

Console path:

Setup > **WLAN-Management**

Possible values:

Syntax:

```
do Disconnect-AP <WTP-MAC>
```

2.37.10.1 E-mail

Activates notification by e-mail.

Console path:

Setup > **WLAN-Management** > **Notification**

Possible values:

No
Yes

Default:

No

2.37.10.2 Syslog

Activates notification by SYSLOG.

Console path:

Setup > **WLAN-Management** > **Notification**

Possible values:

No
Yes

Default:

No

2.37.10.3 E-Mail-Receiver

Information about events in the WLC is sent to this e-mail address.

An SMTP account must be set up to make use of e-mail messaging.

Console path:

Setup > **WLAN-Management** > **Notification**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.37.10.4 Advanced

Here you define the events that you wish to be informed of.

Console path:

Setup > **WLAN-Management** > **Notification**

2.37.10.4.1 Name

Selects the events that trigger notification.

Value is fixed.

Console path:

Setup > **WLAN-Management** > **Notification** > **Advanced**

Possible values:

E-mail
Syslog

2.37.10.4.2 Aktive-Radios

Activates notification about active APs.

Console path:

Setup > **WLAN-Management** > **Notification** > **Advanced**

Possible values:

Yes
No

Default:

No

2.37.10.4.3 Missing-AP

Activates notification about active APs.

Console path:

Setup > **WLAN-Management** > **Notification** > **Advanced**

Possible values:

Yes
No

Default:

No

2.37.10.4.4 New-AP

Activates notification about new APs.

Console path:

Setup > **WLAN-Management** > **Notification** > **Advanced**

Possible values:

Yes
No

Default:

No

2.37.10.5 Send-SNMP-Trap-for-Station-Table-Event

Here you specify when you receive information about events relating to entries in the station table.

Console path:

Setup > **WLAN-Management** > **Notification**

Possible values:

Add/remove_entry
All_events

Default:

Add/remove_entry

2.37.19 Start-automatic-radio-field-optimization

Launches RF optimization automatically. Optimization may be limited to one AP by specifying its MAC address as a parameter.

Console path:

Setup > **WLAN-Management**

Possible values:

Syntax

```
do Start-automatic-radio-field-optimization [<WTP-MAC>]
```

2.37.21 Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

Console path:

Setup > **WLAN-Management**

2.37.21.1 MAC address pattern

Enter the MAC address of a station.

It is possible to use wildcards.

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Possible arguments:

MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

It is possible to use wildcards.

2.37.21.2 Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.21.3 Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 30 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.21.4 WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

This field has no significance for networks secured by WEP.

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.37.21.5 Tx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

2.37.21.6 Rx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

2.37.21.7 VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here. Consequently the client can only be reached by packets originating from the same VLAN. Packets sent by the client are marked with this VLAN ID. You only need to set this value if you want this client to belong to a different VLAN than the logical WLAN (SSID) that it is connected to. 0 means that the client belongs to the VLAN of its logical WLAN (SSID), if this belongs to a VLAN at all.

If you use IPv6, or if multicast is operating on a VLAN, different group keys must be assigned to the different VLANs of an SSID. Otherwise the different multicasts are not be assigned to the correct clients. When using IPv6, for example, clients are informed of IPv6 prefixes that do not function on the VLAN ID.

Console path:

Setup > **WLAN-Management** > **Access-Rules**

Possible values:

Max. 4 characters from `0123456789`

0 … 4096

Default:

0

Special values:

0

No limit

2.37.21.9 SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.

The use of wildcards makes it possible to allow access to multiple SSIDs.

Console path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Special values:

*****

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

empty

2.37.27 Central-Firmware-Management

This menu contains the configuration of central firmware management.

Console path:

Setup > **WLAN-Management**

2.37.27.11 Firmware-Depot-URL

Directory where the latest firmware files are stored. Specify a URL in the form `Server/Directory` or `http://Server/Directory`.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.27.12 Script-Depot-URL

The path to the directory with the script files. Specify a URL in the form `Server/Directory` or `http://Server/Directory`.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.27.13 Update-Firmware-and-Script-Information

Launches an update process for the available firmware and script information with a `do` command.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Syntax

```
do Update-Firmware-and-Script-Information
```

2.37.27.14 Maximum-Number-Of-Loaded-Firmwares

Maximum number of firmware versions in memory

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

1 … 10

Default:

5

2.37.27.15 Firmware-Version-Management

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

2.37.27.15.2 Device

Select here the type of device that the firmware version specified here is to be used for.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Firmware-Version-Management**

Possible values:

All devices
Select from the list of available device types.

Default:

All devices

2.37.27.15.3 MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Firmware-Version-Management**

Possible values:

Max. 12 characters from `[A-Z][a-z][0-9]`

Default:

empty

2.37.27.15.4 Version

Firmware version to be used for the devices or device types specified in this entry. If necessary, an update for the specified devices or device types will be made to this firmware version. This is stated in the form: “xx.yy”, e.g. 10.40.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Firmware-Version-Management**

Possible values:

Max. 5 characters from `[0-9].`

Default:

empty

2.37.27.15.5 Date

Date of the corresponding firmware version.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Firmware-Version-Management**

Possible values:

Max. 8 characters from `[0-9]`

Default:

Corresponds to the UPX header of the firmware (such as "01072014" for the July 01, 2014)

2.37.27.16 Script-Management

Table with the name of the script file and a WLAN profile for allocating the script to a WLAN profile.

Configuring a WLAN router and AP in the Managed mode is handled via WLAN profiles. A script can be used for setting those detailed parameters in managed devices that are not handled by the pre-defined parameters in a WLAN profile. Distribution is also handled by WLAN profiles to ensure that the wireless routers and APs with the same WLC configuration also use the same script.

As only one script file can be defined per WLAN profile, versioning is not possible here. However, when distributing a script to a wireless router or AP, an MD5 checksum of the script file is saved. This checksum allows the WLC to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

2.37.27.16.1 Profile

Select here the WLAN profile that the script file specified here should be used for.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.27.16.2 Name

Enter the CAPWAP slot you selected for the script upload to the WLAN controller (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs). If the WLAN controller obtains the script from a web server, the script name on the web server has to be entered. Possible values: File name in the form `*.lcs`.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.37.27.16.3 Firmware version

Use this item to set the firmware version for which the corresponding script is to be rolled out.

Please enter the firmware version in the form **xx.yy**, e.g. 10.00 or 9.24.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

Possible values:

Max. 6 characters from `[0-9].`

Default:

empty

2.37.27.18 Reboot-updated-APs

Reboot updated APs by means of the `do` command.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Syntax

```
do Reboot-updated-APs
```

2.37.27.25 Firmware-Loopback-Address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If the list of IP networks or loopback addresses contains an entry named "DMZ", the associated IP address will be used.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Name of a defined IP network.
"INT" for the IP address in the first network with the setting "Intranet".
"DMZ" for the IP address in the first network with the setting "DMZ".
Name of a loopback address.
Any other IP address.

2.37.27.26 Script-Loopback-Address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If the list of IP networks or loopback addresses contains an entry named "DMZ", the associated IP address will be used.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

Name of a defined IP network.
"INT" for the IP address in the first network with the setting "Intranet".
"DMZ" for the IP address in the first network with the setting "DMZ".
Name of a loopback address.
Any other IP address.

2.37.27.38 Max. number of concurrent updates

Here you specify how many firmware updates the WLC may perform at the same time.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

1-30
10

Default:

10

2.37.27.39 SSL

This menu contains the encryption parameters for the central firmware management.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

2.37.27.39.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

2.37.27.39.2 Key-exchange algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.37.27.39.3 Crypto-Algorithms

This entry specifies which cryptographic algorithms are allowed.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.37.27.39.4 Hash algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.37.27.39.5 Prefer PFS

This option means that your device always prefers to connect with PFS (Perfect Forward Secrecy), regardless of the default setting of the client.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.37.27.39.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.37.27.39.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

secp256r1

secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.37.27.39.21 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.37.29 Allow WAN connections

This item configures the way that the WLC handles requests from the WAN. For example, it is desirable to prevent CAPWAP requests from unknown WAN peers from accidentally assigning a default configuration with internal network settings to these APs.

Console path:

Setup > **WLAN-Management**

Possible values:

Yes

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration.

VPN

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration only if the WAN connection uses a VPN tunnel.

No

When an AP sends a request from the WAN, the WLC does not include it into the AP management.

Default:

No

2.37.30 Sync-WTP-Password

Activating this function sets the main device password for the AP each time it registers. This ensures that the password is synchronized with that of the WLC. If this function is deactivated, the main device password will only be set if the AP has no password when it registers. Once a password is set, it will not be overwritten.

Console path:

Setup > **WLAN-Management**

Possible values:

Yes
No

Default:

Yes

2.37.31 Interval-for-status-table-cleanup

The WLC regularly cleans up the status tables for the background scans and for the wireless clients. During this cleanup, the WLC removes all entries that are older than the interval in minutes defined here.

Console path:

Setup > **WLAN-Management**

Possible values:

Max. 11 characters from `[0-9]`

Default:

1440

2.37.32 License count

This value indicates the current number of licenses for the WLC that you can use on this device.

This value is for your information only. You cannot change it.

Console path:

Setup > **WLAN-Management**

2.37.33 License limit

This value indicates the maximum possible number of licenses for the WLC that you can use on this device.

This value is for your information only. You cannot change it.

Console path:

Setup > **WLAN-Management**

2.37.34 WLC cluster

This menu contains the settings for the data connections and status connections between multiple WLCs (WLC cluster).

Console path:

Setup > **WLAN-Management**

2.37.34.2 WLC-Data-Tunnel-active

This option activates or disables the use of data tunnels (L3 tunnels) between multiple WLCs. This allows you to extend a transparent layer-2 network as an overlay network across the remote WLCs.

Be sure never to bridge the corresponding WLC tunnels if the individual WLCs are located in the same broadcast domain. Otherwise you will create a switching loop that will overload your network.

In order to maximize data throughput and the network performance, you can forward the AP data traffic directly into the LAN. In this case there is no need for a layer-3 tunnel between the WLCs even when they are in different layer-2 networks.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

Possible values:

Yes

The WLC connects to remote WLCs via a layer-3 tunnel.

No

The WLC does not connect to remote WLCs via a layer-3 tunnel.

Default:

No

2.37.34.3 Static WLC list

In this table, you define the static IPv4 addresses of the remote WLCs which your WLC connects to. As an alternative, this table can also be used to bypass the search of the local network as performed by the **WLC Discovery** table.

If you connect to a remote WLC at a static IPv4 address, your WLC initially establishes a control tunnel to this remote site. If you have enabled the data tunnel option, your WLC automatically establishes a data tunnel to this remote site.

The WLCs can only interconnect if they have a certificate from the same certificate hierarchy.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

2.37.34.3.1 IP address

Here you specify the IPv4 address of the remote WLC to which your WLC establishes a connection.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **Static-WLC-List**

Possible values:

0.0.0.0 … 255,255,255,255

Default:

empty

2.37.34.3.2 Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the remote WLC as the sender.

By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, these will be used on the remote client. **unmasked** !

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **Static-WLC-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Special values:

Name of the IP network (ARF network), whose address should be used.
`INT` for the address of the first Intranet

`DMZ` for the address of the first DMZ

If the lists of IP networks or loopback addresses contains an interface named 'DMZ', then the device selects the associated IP address instead!

`LB0`…`LBF` for one of the 16 loopback addresses or its name

Any IPv4 address

Default:

empty

2.37.34.3.3 Port

Specify the port used by your WLC to establish a data tunnel to the remote WLC.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **Static-WLC-List**

Possible values:

0 … 65535

Special values:

0

The device uses default port 1027.

Default:

0

2.37.34.4 WLC-Discovery

This table is used to enable or disable the automatic search for WLCs in the same local network for each of your IPv4 networks.

Enter the addresses of WLCs that are not on the local network (remote WLCs) into the static WLC list (SNMP ID *2.37.34.3*). The automatic search does not find remote WLCs.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

2.37.34.4.1 Network

Specify the name of the IPv4 network, in which the WLC automatically searches for remote WLCs.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Possible values:

Network name from **Setup** > **TCP-IP** > **Network-list**

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.34.4.2 Operating

Using this option, you can enable or disable the automatic search for remote WLCs in the selected network.

The automatic search for remote WLCs is one way of establishing the connection between several WLCs. If you disable this option, the WLC cannot automatically connect to another WLC over the corresponding network, even if the use of WLC tunnels in general has been enabled. An alternative is to specify the remote sites in the static WLC list.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Possible values:

Yes
No

Default:

No

2.37.34.4.3 Port

Specify the port used for the automatic search for remote WLCs.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Possible values:

0 … 65535

Special values:

0

The device uses default port 1027.

Default:

0

2.37.34.5 Trigger-WLC-rediscovery-on-WTPs

With this action, you command all of the managed APs to calculate the ideal distribution of the APs in the WLC cluster. The result of this calculation may cause the APs to be redistributed.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

Possible arguments:

none

2.37.34.6 WLC-Tunnel-active

Using this parameter, you can enable or disable the WLC tunnel used for WLC clustering. This indirectly switches the cluster functionality for the corresponding WLC on or off.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

Possible values:

No

WLC cluster tunnels on the device are disabled.

Yes

WLC cluster tunnels on the device are enabled.

Default:

No

2.37.34.7 WTP-WLC-Rediscovery

This entry contains the setup values for **WTP-WLC-Rediscovery**.

Console path:

Setup > **WLAN-Management** > **WLC-Cluster**

2.37.35 RADIUS-Server-Profiles

By default, the WLC forwards requests for account and access administration to the RADIUS server. In order for the APs to contact the RADIUS server directly, you define the necessary RADIUS profiles in this table. When setting up logical wireless networks (SSIDs), you have the option of choosing a separate RADIUS profile for each SSID.

SNMP ID: 2.37.35

Telnet path: /Setup/WLAN-Management

2.37.35.1 Name

Name of the RADIUS profile. This name is used to reference the RADIUS profile in the logical WLAN settings.

SNMP ID: 2.30.3.1

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› Max. 16 characters

Default: Blank

2.37.35.2 Account IP

IP address of the RADIUS server that carries out the accounting of user activities. In the default setting with the IP address of 0.0.0.0, the AP sends RADIUS requests to the WLC.

SNMP ID: 2.37.35.2

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› Valid IP address

Default: 0.0.0.0

2.37.35.3 Account port

Port of the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.3

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› Max. 5 numbers

Default: 1813

2.37.35.4 Account secret

Password for the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.4

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› Max. 32 characters

Default: Blank

2.37.35.5 Account loopback

Here, you can optionally configure a sender address for the RADIUS server that carries out the accounting of user activities. This is used instead of the sender address otherwise selected automatically for the destination address. If you have configured loopback addresses, you can specify them here as sender address.

SNMP ID: 2.37.35.5

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› You can enter an address in various forms:
› Name of the IP networks whose addresses are to be used.
› "INT" for the address of the first intranet.
› "DMZ" for the address of the first DMZ

If there is an interface called "DMZ", its address will be taken in this case.

› LBO…LBF for the 16 loopback addresses.
› Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank

2.37.35.6 Account-Protocol

Protocol for communication between the AP and the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.6

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

› RADSEC
› RADIUS

Default: RADIUS

2.37.35.7 Access IP

IP address of the RADIUS server that authenticates user data. In the default setting with the IP address of 0.0.0.0, the AP sends RADIUS requests to the WLC.

SNMP ID: 2.37.35.7

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Valid IP address

Default: 0.0.0.0

2.37.35.8 Access port

Port of the RADIUS server that authenticates user data.

SNMP ID: 2.37.35.8

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 5 numbers

Default: 1812

2.37.35.9 Access secret

Password for the RADIUS server that authenticates user data.

SNMP ID: 2.37.35.9

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 32 characters

Default: Blank

2.37.35.10 Access loopback

Here, you can optionally configure a sender address for the RADIUS server that authenticates user data. This is used instead of the sender address otherwise selected automatically for the destination address. If you have configured loopback addresses, you can specify them here as sender address.

SNMP ID: 2.37.35.10

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- You can enter an address in various forms:
- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

If there is an interface called "DMZ", its address will be taken in this case.

- LBO…LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank

2.37.35.11 Access-Protocol

Protocol for communication between the WLC and the RADIUS server that authenticates the user data.

SNMP ID: 2.37.35.11

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- RADSEC
- RADIUS

Default: RADIUS

2.37.35.12 Backup

Name of the backup RADIUS profile. This name is used to reference the backup RADIUS profile in the logical WLAN settings. The WLC uses the settings from the backup RADIUS profile when the primary RADIUS server for authentication or accounting does not respond to queries.

SNMP ID: 2.30.3.12

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 16 characters

Default: Blank

2.37.36 CAPWAP-Operating

Enables or disabled the CAPWAP service on your device.

In order to operate multiple WLCs in a cluster, they must all have identical configurations. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master controller's configuration.

Console path:

Setup > **WLAN-Management**

Possible values:

No
Yes

Default:

Yes

2.37.37 Preference

This parameter specifies a preferred value used by an AP to set the priority of a WLC within a WLC cluster. The AP evaluates the preference value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 255

Default:

0

2.37.40 Client Steering

This directory is used to configure the client steering by the WLC.

Console path:

Setup > **WLAN-Management**

2.37.40.11 Trace-Mac

An as aid to troubleshooting, only the MAC address you entered is shown when the trace is enabled (`trace # wlc-steering`).

Console path:

Status > **WLAN-Management** > **Client-Steering**

Possible values:

16 characters from `0123456789abcdef`

Default:

0000000000000000

2.37.40.17 Acquire-statistical-data

Using this parameter, you enable or disable the recording of client-steering statistics. This statistical data is suitable for analysis by LANmonitor, for example. Another option for viewing the statistics is available under **Status** > **WLAN-Management** > **Client-Steering**.

Statistics capture increases the load on the WLC. LANCOM does not recommend the permanent recording of statistics.

Console path:

Status > **WLAN-Management** > **Client-Steering**

Possible values:

Yes

Enables the recording of client-steering statistics.

No

Disables the recording of client-steering statistics.

Default:

No

2.37.40.19 Profiles

This table is used to manage the profiles for the client steering. A client-steering profile specifies the conditions under which the WLC triggers a client-steering operation.

Console path:

Status > **WLAN-Management** > **Client-Steering**

2.37.40.19.1 Name

Name of the client-steering profile.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.37.40.19.2 Tolerance level

The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 100 Percent

Default:

0

2.37.40.19.4 Signal-Strength-Weighting

Specifies the percentage weighting of the signal-strength value used to calculate the final value.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 100 Percent

Default:

100

2.37.40.19.5 Associated-Clients-Weighting

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 100 Percent

Default:

100

2.37.40.19.6 Frequency-Band-Weighting

Specifies the percent weighting of the value for the frequency band used to calculate the final value.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 100 Percent

Default:

100

2.37.40.19.9 Preferred-Band

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

2.4GHz

The WLC steers the AP to the 2.4 GHz frequency band.

5GHz

The WLC steers the AP to the 5 GHz frequency band.

Default:

5GHz

2.37.40.19.10 Disassociation-Threshold

Specifies the threshold value below which the connection to the client must drop before the AP disconnects from the client and initiates a new client-steering operation.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 100 Percent

Default:

30

2.37.40.19.11 Time-to-Disassociation

Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

Console path:

Setup > **WLAN-Management** > **Client-Steering** > **Profiles**

Possible values:

0 … 10 Seconds

Default:

1

2.37.40.20 Client-MAC-Statistic-Filter

This parameter specifies a list of MAC addresses, for which the WLC explicitly records statistical data. The WLC writes statistics for the listed MAC addresses to the **Event-Table** under **Status** > **WLAN-Management** > **Client-Steering**. Multiple MAC addresses can be specified in a comma-separated list.

The recording of statistical data is enabled elsewhere using the parameter *2.37.40.17 Acquire-statistical-data* on page 1330.

Console path:

Status > **WLAN-Management** > **Client-Steering**

Possible values:

Max. 251 characters from `[0-9][a-f]:-,`

Special values:

empty

The device collects statistical data on all MAC addresses (filtering disabled).

Default:

empty

2.38 LLDP

This submenu contains the configuration options relating to the Link Layer Discovery Protocol (LLDP). The options are similar to the configuration options according to LLDP MIB. If the information contained here is not sufficient, you can find more details in the IEEE 802.1AB standard.

To find out whether a specific device supports LLDP, refer to the corresponding data sheet.

Console path:

Setup

2.38.1 Message-TX-Interval

This value defines the interval in seconds for the regular transmission of LLDPDUs by the device.

If the device detects changes to the LLDP information during an interval, the device can send additional LLDP messages. The *2.38.4 TX delay* on page 1335 parameter defines the maximum frequency of LLDP messages caused by these changes.

The device also uses this `Message TX interval` for calculating the hold time for received LLDP messages with the help of the *Message TX hold multiplier*.

Console path:

Setup > **LLDP**

Possible values:

0 … 65535 Seconds

Default:

30

2.38.2 Message-Tx-Hold-Multiplier

This value is used to calculate the time in seconds after which the device discards the information received with LLDP messages (hold time or time to live – TTL). The device calculates this value as the product of the `Message TX hold multiplier` specified here and the current *Message TX interval*:

Hold time = `Message-Tx-Hold-Multiplier` x `Message-TX-Interval`

The default settings result in a hold time for received LLDP messages of 120 seconds.

Console path:

Setup > **LLDP**

Possible values:

0 … 99 Seconds

Default:

4

2.38.3 Reinit-Delay

This value defines the time the device suppresses transmission of LLDPDUs even though the LLDP is activated.

Console path:

Setup > **LLDP**

Possible values:

0 … 99 Seconds

Default:

2

2.38.4 TX delay

In principle the device sends LLDP messages in the interval set under *Message TX interval*. If the device detects changes to the LLDP information during an interval, the device can send additional LLDP messages.

The value set here defines the maximum frequency in seconds, in which the device uses LLDP messages. Thus the default value of 2 seconds causes the device to send LLDP messages once every 2 seconds, even if the device has detected multiple changes in the meantime.

Console path:

Setup > **LLDP**

Possible values:

0 … 9999 Seconds

Default:

2

2.38.5 Notification-Interval

This value specifies the time interval until the device sends notifications of changes to the remote station tables. The value defines the smallest time period between notifications. Thus the default value of 5 seconds causes the device to send messages at most once every 5 seconds, even if the device has detected multiple changes in the meantime.

Console path:

Setup > **LLDP**

Possible values:

0 … 9999 Seconds

Default:

5

2.38.6 Ports

This table includes all port-dependent configuration options. The table index is a string, specifically the interface/port name.

Console path:

Setup > **LLDP**

2.38.6.1 Name

The name of the port or interface, which depends on the available interfaces (e.g. LAN-1, WLAN-1).

Console path:

Setup > **LLDP** > **Ports**

2.38.6.2 Admin-Status

Specifies whether PDU transfer and/or reception is active or inactive on this port. This parameter can be set individually for each port.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

Off
Rx-Only
Rx/Tx

Default:

Off

2.38.6.3 Notifications

Use this to set whether changes in an MSAP remote station for this port are reported to possible network management systems.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

No
Yes

Default:

No

2.38.6.4 TLVs

Specify the quantity of the optional standard TLVs that will be transmitted to the PDUs.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

Port-Description
Sys-Name
Sys-Descriptor
Sys-Caps
None

Default:

Port-Description

2.38.6.6 TLVs-802.3

Specify the quantity of the optional standard TLVs-802.3 that will be transmitted to the PDUs.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

PHY-Config-Status
Power-via-MDI
Link-Aggregation
Max-Frame-Size
None

Default:

PHY-Config-Status

2.38.6.7 Max-Neighbours

This parameter specifies the maximum number of LLDP neighbors.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

0 … 65535

Default:

0

2.38.6.8 Update-Source

This parameter specifies the optional sources for LLDP updates.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

Auto
LLDP-Only
Other only
Both

Default:

Auto

2.38.6.9 TLVs-LCS

These settings define the quantity of the optional standard LCS TLVs that the device sends to PDUs.

Console path:

Setup > **LLDP** > **Ports**

Possible values:

SSID
Radio channel
PHY-Type
None

Default:

SSID

2.38.7 Management-Addresses

In this table, enter the management address(es) that the device transmits via LLDPDUs. Management addresses take their names from the TCP/IP network list. The device only transfers the network and management addresses in this table for the LLDPDUs. A network from this list has the option of using the port list to limit the wider disclosure of the individual device addresses.

Defining address bindings limits the disclosure of management addresses regardless of the settings in the port lists. The device only reports a network that is connected to an interface. This is irrespective of the settings of the port list.

Console path:

Setup > **LLDP**

2.38.7.1 Network name

The name of the TCP/IP network, as entered in the TCP-IP network list.

Console path:

Setup > **LLDP** > **Management-Addresses**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.38.7.2 Port-List

The list of interfaces and ports belonging to the corresponding management address.

You have the option to specify a comma-separated list of ports, e.g. LAN-1,LAN-2, or WLAN-1,WLAN-2. Use wildcards to specify a group of ports (e.g., "*_*").

Console path:

Setup > **LLDP** > **Management-Addresses**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.38.8 Protocols

This table contains the LLDP port settings for the spanning-tree and rapid-spanning-tree protocols.

Console path:

Setup > **LLDP**

2.38.8.1 Protocol

This parameter sets the protocol for which the LLDP ports are enabled.

Console path:

Setup > **LLDP** > **Protocols**

Possible values:

Spanning-Tree
Rapid Spanning Tree

Default:

Spanning-Tree

Rapid Spanning Tree

2.38.8.2 Port-List

This value describes the ports, which the LLDP uses with the associated protocol (spanning-tree or rapid-spanning-tree).

You have the option to specify a comma-separated list of ports, e.g. LAN-1,LAN-2, or WLAN-1,WLAN-2. Use wildcards to specify a group of ports (e.g., "*_*").

Console path:

Setup > **LLDP** > **Protocols**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.38.9 Immediate delete

This parameter enables or disables the direct deletion of LLDPDUs.

Console path:

Setup > **LLDP**

Possible values:

No
Yes

Default:

Yes

2.38.10 Operating

This parameter enables or disables the use of LLDP.

Console path:

Setup > **LLDP**

Possible values:

No
Yes

Default:

Yes

2.39 Certificates

This menu contains the configuration of the certificates.

Console path:

Setup

2.39.1 SCEP-Client

This menu contains the configuration of the SCEP client.

Console path:

Setup > **Certificates**

2.39.1.1 Operating

Turns the usage of SCEP on or off.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

No
Yes

Default:

No

2.39.1.2 Device-Certificate-Update-Before

Preparation time in days for the timely retrieval of new RA/CA certificates.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

2

2.39.1.3 CA-Certificate-Update-Before

Preparation time in days for the timely retrieval of new RA/CA certificates.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.39.1.7 Certificates

Here you can configure certificates or add new ones.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3

2.39.1.7.1 Name

The certificate's configuration name.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.39.1.7.2 CADN

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

Comma

(",")

Slash

("/")

Plus

("+")

Semicolon

(";")

Equals

("=")

You can also use the following internal LCOS variables:

Variable	Meaning
%%	Inserts a percent sign.
%f	Inserts the version and the date of the firmware currently active in the device.
%r	Inserts the hardware release of the device.
%v	Inserts the version of the loader currently active in the device.
%m	Inserts the MAC address of the device.
%s	Inserts the device serial number.
%n	Inserts the name of the device.

Variable	Meaning
%l	Inserts the location of the device.
%d	Inserts the type of the device.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.7.3 Subject

Distinguished name of the subject of the requester.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

Comma

(",")

Slash

("/")

Plus

("+")

Semicolon

(";")

Equals

("=")

You can also use the following internal LCOS variables:

Variable	Meaning
%%	Inserts a percent sign.
%f	Inserts the version and the date of the firmware currently active in the device.
%r	Inserts the hardware release of the device.
%v	Inserts the version of the loader currently active in the device.
%m	Inserts the MAC address of the device.
%s	Inserts the device serial number.
%n	Inserts the name of the device.
%l	Inserts the location of the device.
%d	Inserts the type of the device.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.7.4 ChallengePwd

Password (for the automatic issue of device certificates on the SCEP server).

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.7.5 SubjectAltName

Further information about the requester, e.g. domain or IP address.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.7.6 KeyUsage

Any comma-separated combination of: `digitalSignature`, `nonRepudiation`, `keyEncipherment`, `dataEncipherment`, `keyAgreement`, `keyCertSign`, `cRLSign`, `encipherOnly`, `decipherOnly`, `critical` (possible but not recommended).

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.7.7 Device-Certificate-Keylength

The length of the key to be generated for the device itself.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.39.1.7.8 Application

Indicates the intended application of the specified certificates. The certificates entered here are only queried for the corresponding application.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

VPN1
VPN2
VPN3
VPN4
VPN5
VPN6
VPN7
VPN8
VPN9
WLan-Controller
EAP/TLS
Default
CA
ConfigSync
unconfigured

Default:

VPN1

2.39.1.7.9 Extended-KeyUsage

Any comma-separated combination of: `critical`, `serverAuth`, `clientAuth`, `codeSigning`, `emailProtection`, `timeStamping`, `msCodeInd`, `msCodeCom`, `msCTLSign`, `msSGC`, `msEFS`, `nsSGC`, `1.3.6.1.5.5.7.3.18` for WLAN controllers, `1.3.6.1.5.5.7.3.19` for access points in managed mode.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.8 Reinit

Starts the manual reinitialization of the SCEP parameters. As with the standard SCEP initialization, the necessary RA and CA certificates are retrieved from the CA and stored within the device's file system so that they are not yet ready for use in VPN operations. If the available system certificate fits to the retrieved CA certificate, then the system certificate, CA certificate and the device's private key can be used for VPN operations. If the existing system certificates do not fit to the retrieved CA certificate, then the next step is for the SCEP server to submit a new certificate request. Only once a new system certificate that fits to the retrieved CA certificate has been issued and retrieved can the system certificate, CA certificate and the device's private key can be used for VPN operations.

SNMP ID: 2.39.1.8

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.9 Update

Manually triggers a request for a new system certificate, irrespective of the remaining validity period (lease). A new key pair is generated at the same time.

SNMP ID: 2.39.1.9

Telnet path: /Setup/Certificates/SCEP-Client

2.39.1.10 Clear-SCEP-Filesystem

Starts a clean-up of the SCEP file system.

Deleted are: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.

Retained are: System certificates currently in use for VPN operations, associated private keys, and the CA certificates currently in use for VPN operations.

Console path:

Setup > **Certificates** > **SCEP-Client**

2.39.1.11 Retry-After-Error-Interval

Interval in seconds between retries after errors of any type.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

22

2.39.1.12 Check-Pending-Requests-Interval

Interval in seconds for checks on outstanding certificate requests.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

101

2.39.1.13 Trace level

The output of trace messages for the SCEP client trace can be restricted to contain certain content only. The specified value defines the amount of detail of the packets in the trace.

Console path:

Setup > **Certificates** > **SCEP-Client**

Possible values:

All

All trace messages are output, including information and debug messages.

Reduced

Only error and alert messages are output.

Only errors

Only error messages are output.

Default:

All

Reduced

2.39.1.14 CAs

This table is used to define the available CAs.

Console path:

Setup > **Certificates** > **SCEP-Client**

2.39.1.14.1 Name

Enter a name that identifies this configuration.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.39.1.14.2 URL

This is where the enrollment URL is entered. The router must contact the certificate authority (CA) to request a certificate. The URL required tends to differ from one provider to another, and it is commonly specified in the documentation of the CA. Example: `http:/ /postman/certsrv/mscep/mscep.dll>`

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.39.1.14.3 DN

The distinguished name is entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway.

The following are examples of how an entry might appear: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM Systems/C=DE`

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

Comma

(",")

Slash

("/")

Plus

("+")

Semicolon

(";")

Equals

("=")

You can also use the following internal LCOS variables:

Variable	Meaning
%%	Inserts a percent sign.
%f	Inserts the version and the date of the firmware currently active in the device.
%r	Inserts the hardware release of the device.
%v	Inserts the version of the loader currently active in the device.
%m	Inserts the MAC address of the device.
%s	Inserts the device serial number.
%n	Inserts the name of the device.
%l	Inserts the location of the device.
%d	Inserts the type of the device.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.14.4 Enc-Alg

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:

If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

DES

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

2.39.1.14.5 Identifier

An additional identifier can be specified here. This value is required by some web servers to identify the CA.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.14.6 CA signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

2.39.1.14.7 RA autoapprove

With this option, new requests are signed with this assuming that a system certificate is available. The option must be activated both at the client and at the Certificate Authority (CA server). In this case the client is authenticated at the CA by the certificate alone and without exchange of a challenge password.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

No
Yes

Default:

No

2.39.1.14.8 CA fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Off
MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

2.39.1.14.9 CA-Fingerprint

The CA fingerprint can be entered here. This is a hash value that is produced by the fingerprint algorithm. This hash value can be used to check the authenticity of the received CA certificate (if a CA fingerprint algorithm is a requirement). Possible delimiters are: " :" " -" " ," "[Space]".

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 59 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.1.14.11 Loopback-Addr.

Enter a loopback address.

Console path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.39.1.17 Logging

This menu contains settings for the logging.

Console path:

Setup > **Certificates** > **SCEP-Client**

2.39.1.17.1 E-mail

This entry contains the setup values for e-mail.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Logging**

2.39.1.17.2 Syslog

This entry contains the setup values for Syslog.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Logging**

2.39.1.17.3 E-mail recipient

This entry contains the setup values for the e-mail recipient.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Logging**

2.39.1.17.4 Expiration-Reminder-before

This entry contains the setup values for Expiration-Reminder-before.

Console path:

Setup > **Certificates** > **SCEP-Client** > **Logging**

2.39.2 SCEP-CA

This menu contains the settings for SCEP-CA.

Console path:

Setup > **Certificates** > **SCEP-Client**

2.39.2.1 Operating

Activates or deactivates the SCEP client.

Console path:

Setup > **Certificates** > **SCEP-Client** > **SCEP-CA**

Possible values:

No
Yes

Default:

No

2.39.2.2 CA-certificates

This menu contains the settings for CA certificates.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.2.1 CA Distinguished Name

The "distinguished name" is entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE`.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.2.3 Alternative name

An alternative "Subject Name" can be entered here.

Example:

```
critical,DNS:host.company.de   IP:10.10.10.10   DNS:host.company.de,
IP:10.10.10.10 UFQDN:email:name@company.de
```

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.2.4 RSA key length

The key length must be entered here. This value specifies the length of new keys in bits.

The time taken for calculation depends on the performance available from the system; the greater the number of bits, the longer it takes.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

1024
2048
3072
4096
8192

Default:

2048

2.39.2.2.5 Validity period

Here you enter the certificate's validity period in days.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1100

2.39.2.2.6 Update-CA-certificates-before-expiration

Enter the time period for the "Update before expiry" in days.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

Max. 2 characters from `[0-9]`

Default:

4

2.39.2.2.8 RA distinguished name

The "distinguished name" is entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE`

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.2.9 Create new CA certificates

Run this command if you have changed the configuration of the CA.

The CA only creates new certificates automatically when the old ones have expired or none are available. If you decide to change the key length, the name, or other values of the CA certificate, this command enables you to recreate the corresponding certificate files.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

2.39.2.2.10 Create PKCS12 backup files

To restore the CA or RA, the relevant root certificates with private keys will be required that are generated automatically when the WLC is started.

To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PCKS12 container.

The command "Create-PKCS12-Backup-Files" starts the export. Enter the passphrase when prompted to enter a parameter.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

2.39.2.2.11 Restore-certificates-from-Backup

In case of a backup event, this command restores the two PKCS12 files with their respective root certificates and the private keys from the CA and/or RA.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates**

2.39.2.3 Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:

If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

DES

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default:

DES

2.39.2.4 RA-Autoapprove

With this option, new requests are signed with this assuming that a system certificate is available. The option must be activated both at the client and at the Certificate Authority (CA server). In this case the client is authenticated at the CA by the certificate alone and without exchange of a challenge password.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

No
Yes

Default:

Yes

2.39.2.5 Client certificates

This menu contains the settings for client certificates.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.5.1 Validity period

Here you specify the validity period of the certificate in days.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Client-Certificates**

Possible values:

Max. 5 characters from `[0-9]`

Default:

365

2.39.2.5.3 Challenge passwords

This table provides an overview of the challenge passwords.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Client-Certificates**

2.39.2.5.3.1 Index

Enter the index for the challenge password here.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

Max. 10 characters from `0123456789`

Default:

empty

2.39.2.5.3.2 Subject-Distinguished-Name

The "Distinguished name" must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE`

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.5.3.3 MAC address

Enter the MAC address of the client whose password is to be managed by the challenge-password table.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

Max. 12 characters from `0123456789abcdef`

Default:

empty

2.39.2.5.3.4 Challenge

Enter the challenge (password) for the client here.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.39.2.5.3.5 Challenge

The validity of the password is fixed as “permanent”.

Enter the validity period of the password here. By selecting “one-time” the password becomes a one-time password (OTP), so it can only be used for authentication once.

Console path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

Permanent

Default:

Permanent

Possible values:

One-time
Permanent

Default:

Permanent

2.39.2.5.4 General-challenge-password

An additional 'password' can be entered here, which is transmitted to the CA. This can be used by default to authenticate revocation requests. If CAs operate Microsoft-SCEP (mscep), the one-time passwords issued by the CA can be entered here for the authentication of requests.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Client-Certificates**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.39.2.6 Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

2.39.2.7 Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

2.39.2.8 Certificate revocation lists

This item contains the certificate revocation lists.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.8.1 Update interval

Enter here the update interval in seconds for creating a new CRL. The lower limit for this is 600 seconds.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Certificate-Revocation-Lists**

Possible values:

Max. 63 characters from `[0-9]`

Default:

86400

2.39.2.8.2 CRL-Distribution-Point-Hostname

The parameter specifies the name of the CRL distribution point as the IP address or FQDN where this device is to be reached. The CA automatically extends the parameter to the appropriate URL.

The URL of the CRL distribution point appears in certificates issued by the CA.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Certificate-Revocation-Lists**

Possible values:

String

Default:

empty

2.39.2.8.3 Create-new-CRL

Normally, the CA automatically creates a new certificate revocation list (CRL) when the old CRL expires or when the contents of the CRL changes (due to SCEP operations).

Run this command if you have revoked a certificate in the certificate status list.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Certificate-Revocation-Lists**

2.39.2.9 Reinitialize

Use this command to reinitialize the CA. The device checks the configuration and the certificates, and if necessary it updates the corresponding values and files.

Run this command when the CA is not running because of a configuration error. This initiates a new check after a change of configuration.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.10 News

This menu contains the settings for the notification of events relating to certificates.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.10.1 E-mail

The setting here determines whether a notification is sent when an event occurs.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Notification**

Possible values:

No
Yes

Default:

No

2.39.2.10.2 Syslog

This item activates the logging function based on notifications via Syslog.

To make use of this function, the Syslog client in the device needs to be configured accordingly.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Notification**

Possible values:

No
Yes

Default:

No

2.39.2.10.3 E-Mail-Receiver

Here you enter the e-mail address to which a notification is sent when an event occurs.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Notification**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.10.4 Send-Backup-Reminder

If this function is activated, a reminder about the need to make a backup is sent automatically to the e-mail address entered here.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Notification**

Possible values:

No
Yes

Default:

No

2.39.2.11 Root-CA

This parameter specifies whether or not the CA of the relevant WLC represents the root CA.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

No
Yes

Default:

Yes

2.39.2.12 CA-Path-Length

Use this parameter to specify the maximum permitted length of the hierarchy of sub-CAs below the root CA (length of the "chain of trust").

A value of `1` means that only the root CA can issue certificates for sub-CAs. Sub-CAs themselves cannot issue certificates to other sub-CAs and so extend the "chain of trust". When set to `0`, not even the root CA is capable of issuing certificates for sub-CAs. In this case, the root CA can only sign end-user certificates.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

0 … 65535

Default:

1

2.39.2.13 Sub-CA

This menu contains all of the settings you need for retrieving a certificate for the sub-CA.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.13.1 Auto-generated-Request

With this parameter you specify whether the WLC forwards the request for a certificate for the sub-CA automatically to the root CA.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

No
Yes

Default:

No

2.39.2.13.2 CADN

Enter the certificate authority distinguished name (CADN) of the parent CA (e.g. the root CA) where the WLC obtains the certificate for the sub-CA.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

Max. 100 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.39.2.13.3 Challenge-Pwd

Set the challenge password used by the sub-CA to obtain the certificate from the parent CA (e.g., the root CA). You set the challenge password for the parent CA in LCOS in the menu **Setup** > **Certificates** > **SCEP-CA** > **Client-Certificates**.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

Max. 100 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

2.39.2.13.4 Ext-Key-Usage

With this item you specify additional designated purposes for the key usage. The extended key usage consists of a comma-separated list of key usages. These indicate the purposes for which the certificate's public key may be used.

The purposes are entered either as their abbreviations or the dot-separated form of the OIDs. Although any OID can be used, only a few of them are meaningful (see below). Specifically the following PKIX, NS and MS values are significant and can be entered in any combination:

Table 16: Extended usage: Meaningful abbreviations

Value	Meaning
serverAuth	SSL/TLS Web server authentication
clientAuth	SSL/TLS Web client authentication
codeSigning	Code signing
emailProtection	E-mail protection (S/MIME)
timeStamping	Trusted time stamping
msCodeInd	Microsoft personal code signing (Authenticode)
msCodeCom	Microsoft commercial code signing (Authenticode)
msCTLSign	Microsoft trust list signing
msSGC	Microsoft server gated crypto
msEFS	Microsoft encrypted file system
nsSGC	Netscape server gated crypto
critical	By setting this restriction, the key usage extension must always be observed. If the extension is not supported, the certificate is rejected as invalid.

Table 17: Extended usage: Meaningful OIDs for WLAN switching

Device	OID
WLC	1.3.6.1.5.5.7.3.18
Managed AP	1.3.6.1.5.5.7.3.19

Sample input: `critical,clientAuth,1.3.6.1.5.5.7.3.19`

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

Comma separated list of the abbreviations and/or OIDs listed above. Max. 100 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.13.5 Cert-Key-Usage

Specify the intended application of the specified certificates (key usage). The WLC queries the certificates for the sub-CA only for the purpose indicated.

Table 18: Usage: Abbreviation

Value	Meaning
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
encipherOnly	
decipherOnly	
critical	By setting this restriction, the key usage extension must always be observed. If the extension is not supported, the certificate is rejected as invalid.

Sample input: `digitalSignature, nonRepudiation`

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

Comma separated list of the abbreviations listed above. Max. 100 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.13.8 CA-Url-Address

Specify the URL (address) where the parent CA is to be found. If another WLC with the LCOS operating system provides the CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Sub-CA**

Possible values:

Max. 251 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

http://127.0.0.1/cgi-bin/pkiclient.exe

2.39.2.14 Web interface

In this directory, you configure the settings for the SCEP-CA web interface.

Console path:

Setup > **Certificates** > **SCEP-CA**

2.39.2.14.1 Profiles

In this table you create profiles with collected certificate properties.

By default three profiles are already available for common application scenarios.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface**

2.39.2.14.1.1 Profile name

Here you assign a unique name for the profile.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.2 Key usage

Specifies for which application the profile is to be used. The following usages are available:

- critical
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly

Multiple comma-separated entries can be selected.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default:

critical,digitalSignature,keyEncipherment

2.39.2.14.1.3 Extended key usage

Specifies the extended application for which the profile is to be used. The following usages are available:

- critical
- serverAuth: SSL/TLS Web server authentication
- clientAuth: SSL/TLS Web client authentication
- codeSigning: Signing of program code
- emailProtection: E-mail protection (S/MIME)
- timeStamping: Furnishing data with reliable time stamps
- msCodeInd: Microsoft Individual Code Signing (authenticode)
- msCodeCom: Microsoft Commercial Code Signing (authenticode)
- msCTLSign: Microsoft Trust List Signing
- msSGC: Microsoft Server Gated Crypto
- msEFS: Microsoft Encrypted File System
- nsSGC: Netscape Server Gated Crypto

Multiple comma-separated entries can be selected.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.4 RSA key length

Sets the length of the key.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

1024
2048
3072
4096
8192

Default:

2048

2.39.2.14.1.5 Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 10 characters from `0123456789`

Default:

365

2.39.2.14.1.6 CA

Indicates whether this is a CA certificate.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Yes
No

Default:

No

2.39.2.14.1.7 Password

Password to protect the PKCS12 certificate file.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.2.14.1.8 Country

Enter the country identifier (e.g. “DE” for Germany).

This entry appears in the subject or issuer of the certificate under `C=` (**C**ountry).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

2 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.9 Locality name

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under `L=` (**L**ocality).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.10 Organization

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `O=` (**O**rganization).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.11 Organization unit name

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `OU=` (**O**rganization **U**nit).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.12 State or province

Enter the State or province.

This entry appears in the subject or issuer of the certificate under `ST=` (**ST**ate).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.13 E-mail

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 36 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.14 Surname

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN=` (**S**ur**N**ame).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.15 Serial number

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.16 Postal code

Enter the location post code.

This entry appears in the subject or issuer of the certificate under `postalCode=`.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 25 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.17 Template

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Setup** > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.18 Subject-Alternative-Name

Specify the subject alternative name (SAN) here. The SAN contains further information for use by applications.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.1.19 OCSP-AIA

Enter the name or IP address where OCSP clients can reach the OCSP server.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

Default:

empty

2.39.2.14.2 Template

In this table, you define the templates for certificate profiles.

Here you specify which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.

A “Default” template is already available.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface**

2.39.2.14.2.1 Name

Give the template a unique name here.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*-:<>?[\]_.`

Default:

empty

2.39.2.14.2.2 Key usage

Specifies for which application the profile is to be used.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.3 Extended key usage

Specifies the extended application for which the profile is to be used.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.4 RSA key length

Sets the length of the key.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.5 Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.6 CA

Indicates whether this is a CA certificate.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.8 Country

Specifies the country identifier (e.g. "DE" for Germany).

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.9 Locality name

Specifies the locality.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.10 Organization

Specifies the organization issuing the certificate.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.11 Organization unit name

Specifies the unit within the organization that issues the certificate.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.12 State or province

Specifies the State or province.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.13 E-mail

Specifies the e-mail address.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.14 Surname

Specifies the surname.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.15 Serial number

Specifies the serial number.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.16 Postal code

Specifies the postal code.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.17 Subject-Alternative-Name

The "Subject Alternative Name" (SAN) links additional data with this certificate.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.14.2.18 OCSP-AIA

When creating a certificate using Smart Certificate, the field "OCSP AIA" (OCSP Authority Information Access) can be displayed.

Console path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2.39.2.15 RSA-Padding-Method

Specifies the RSA padding method for certificates issued by the SCEP-CA.

Console path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

PKCS1

Certificate padding is performed with the RSASSA-PKCS1-v1_5 method.

PSS

Certificate padding is performed with the RSASSA-PSS method

Default:

PKCS1

2.39.3 CRLs

This menu contains the configuration of the CRLs.

Console path:

Setup > **Certificates**

2.39.3.1 Operating

If enabled, the certificate check also considers the CRL (if available).

If this option is activated but no valid CRL is available (e.g. if the server can't be reached), then all connections will be rejected and existing connections will be interrupted.

Console path:

Setup > **Certificates** > **CRLs**

Possible values:

No
Yes

Default:

No

2.39.3.4 Update-Before

The point in time prior to expiry of the CRL when the new CRL can be loaded. This value is increased by a random value to prevent server overload from multiple simultaneous queries. Once within this time frame, any coinciding regular planned updates will be stopped.

If the first attempt to load the CRL fails, new attempts are made at regular short intervals.

Console path:

Setup > **Certificates** > **CRLs**

Possible values:

Max. 10 characters from `[0-9]`

Default:

300

2.39.3.5 Prefetch-Period

The time period after which periodic attempts are made to retrieve a new CRL. Useful for the early retreival of CRLs published at irregular intervals. The entry "0" disables regular retrieval.

If with regular updates the CRL cannot be retreived, no further attempts will be started until the next regular attempt.

Console path:

Setup > **Certificates** > **CRLs**

Possible values:

Max. 10 characters from `[0-9]`

Default:

300

2.39.3.6 Validity exceedance

Even after expiry of the CRL, certificate-based connections will continue to be accepted for the period defined here. This tolerance period can prevent the unintentional rejection or interruption of connections if the CRL server should be temporarily unavailable.

Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

In the time period defined here, even expired certificates can be used to maintain or re-establish a connection.

Console path:

Setup > **Certificates** > **CRLs**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.39.3.7 Refresh-CRL-Now

Reads the current CRL from the URL specified in the root certificate, or from the alternative URL (if this function is set up).

Console path:

Setup > **Certificates** > **CRLs**

2.39.3.8 Alternative-URL-Table

This table contains the list of alternative URLs.

The address where a certificate revocation list (CRL) can be collected is normally defined in the certificate (as crlDistributionPoint). In LCOS, alternative CRLs can be specified in a table. After a system start the CRLs are automatically collected from these URLs. These are used in addition to the lists offered by the certificates.

Console path:

Setup > **Certificates** > **CRLs**

2.39.3.8.1 Alternative URL

Here you enter the alternative URL where a CRL can be collected.

Console path:

Setup > **Certificates** > **CRLs** > **Alternative-URL-Table**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.3.9 Loopback address

Here you can optionally define a sender address for display to the recipient instead of the automatically generated address.

If there is an interface called "DMZ", its address will be taken if you have selected "DMZ".

Console path:

Setup > **Certificates** > **CRLs**

Possible values:

Name of the IP network whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LBO…LBF for the 16 loopback addresses.
Any IP address in the form `x.x.x.x`.

2.39.6 OCSP-Client

This menu contains the settings for the OCSP client.

SNMP ID: 2.39.6

Telnet path: /Setup/Certificates

2.39.6.1 CA profile table

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Console path:

Setup > **Certificates** > **OCSP-Client**

2.39.6.1.1 Profile name

Enter here the name of a CA profile to be used by the OCSP client for a particular CA.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

Maximum 32 alphanumerical characters

Default:

2.39.6.1.2 CA-DN

Enter the distinguished name of the CA, whose certificates are evaluated by the OCSP client with this profile name.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

Maximum 251 alphanumerical characters

Default:

2.39.6.1.3 Prefer-AIA

Certificates used for establishing VPN connections optionally include the URL of the relevant OCSP responder in the field Authority Info Access (AIA). This item defines whether the OCSP client prefers to use the URL from this entry in the CA profile table or the URL from the AIA field, if available.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

- **No**: The OCSP client always uses the URL from this CA-profile table entry and ignores the URL in the AIA field.
- **Yes**: The OCSP client uses the URL from the AIA field (if specified) and ignores the URL from this CA profile table entry.

Default:

No

2.39.6.1.4 Responder-Profile-Name

This item selects the responder profile used by the OCSP client to evaluate certificates from this CA.

If the field for the responder profile name is left empty, the machine evaluates the certificates from the CA defined here not with OCSP, but with the help of a CRL.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

Select from the list of profile names in the table *Responder profile table*, maximum 32 alphanumeric characters

Default:

2.39.6.1.5 Source interface

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as sender address.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

- Name of the IP network (ARF network), whose address should be used.
- `INT` for the address of the first Intranet
- `DMZ` for the address of the first DMZ

  If the list of IP networks or loopback addresses contains an entry named 'DMZ', then the associated IP address will be used instead.
- `LB0`…`LBF` for one of the 16 loopback addresses or its name
- Any IPv4 address

If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

Default:

0.0.0.0

2.39.6.1.6 Cert-Evaluation-Mode

This item defines how the device behaves if certificate evaluation fails. During connection establishment, the OCSP client first queries the OCSP responder about the validity of the certificate. If the certificate is about to expire, the OCSP client automatically repeats the query about the validity before the certificate expires.

If necessary, you can log and review the results of certificate evaluation by the OCSP responder with SYSLOG, SNMP traps and relevant traces.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

- **Strict**: If the OCSP responder reports that the certificate used during connection establishment is not valid, the device does not establish a connection to the remote site. If during an ongoing connection the OCSP responder does not confirm a new request in good time before the certificate's expiry, the device will cut the connection.
- **Loose**: If the OCSP responder reports that the certificate used during connection establishment is not valid, the device will still establish a connection to the remote site. Even if during an ongoing connection the OCSP responder does not confirm a new request in good time before the certificate's expiry, the device will not cut the connection.

Default:

Strict

2.39.6.1.7 Syslog-Events

The OCSP client can optionally generate SYSLOG messages with information on the results of certificate checks by the OCSP responder.

Telnet path:

Setup > **Certificates** > **OCSP-Client** > **CA-Profile-table**

Possible values:

- **Yes**: The OCSP client creates SYSLOG messages.
- **No**: The OCSP client does not generate SYSLOG messages.

Default:

Yes

2.39.6.2 Responder profile table

This table contains information on the Certificate Authorities (CAs), whose certificates are evaluated by the OCSP client by sending a request to an OCSP responder.

Console path:

Setup > **Certificates** > **OCSP-Client**

2.39.6.2.1 Profile name

Enter here the name of an OCSP-responder profile to be referenced by the OCSP client in the CA profile table.

Console path:

Setup > **Certificates** > **OCSP-Client** > **Responder-Profile-table**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.6.2.2 URL

Enter the URL for the OCSP client to access the OCSP responder.

Console path:

Setup > **Certificates** > **OCSP-Client** > **Responder-Profile-table**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.7 OCSP server

This table contains the settings for the OCSP server.

Console path:

Setup > **Certificates**

2.39.7.1 Operating

Turn the OCSP server on or off here.

Console path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No

Default:

No

2.39.7.2 Port

The port used by the OCSP server.

Console path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

8084

2.39.7.3 Certificate-Subject

Operating the OCSP server requires it to receive a certificate from the certification authority (CA) whose certificates it should provide information about. This certificate is used to sign the OCSP responses. Here you enter the name or IP address where OCSP clients can contact the OCSP server, e.g. `/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE`

In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

Console path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE

2.39.7.4 WAN access

This setting determines if and how the OCSP server can be reached from the WAN.

Console path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No
Over-VPN

Default:

No

2.39.7.5 Signature-Algo

The algorithm used to generate the certificate used by the OCSP server.

Console path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

SHA1
SHA-256
SHA-384
SHA-512

Default:

SHA-256

2.39.8 ACME-Client

This table contains the settings for the ACME client. The Automatic Certificate Management Environment (ACME) client as per *RFC 8555* is supported for Let's Encrypt certificates. *Let's Encrypt* is a free and open certification authority that makes it possible to obtain free SSL/TLS certificates. The certificates can be used for WEBconfig and for the Public Spot.

Console path:

Setup > **Certificates**

2.39.8.1 Endpoint

Endpoint or URL to which the certificate request is addressed.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

Max. 100 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

https://acme-v02.api.letsencrypt.org/directory

2.39.8.2 Domain

DNS domain name for which the certificate is to be created, e.g. “test.example.com”

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

Max. 100 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.8.3 SAN-List

Defines which other domain names should be entered into the SAN field (Subject Alternative Name) of the certificate. This can be a comma-separated list of domain names (without spaces).

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

Max. 200 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.39.8.4 Contact

Defines the contact information for the certificate request, e.g. the e-mail address “test@example.com”.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

Max. 200 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.39.8.5 Endpoint-Resolution

Defines the protocol to be used to resolve the endpoint.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

IPv4-Only
IPv6-Only
IPv6-Or-IPv4

2.39.8.6 Certificate-Type

Defines the certificate type including key length.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

RSA-2K
RSA-3K
RSA-4K
ECC-256
ECC-384

Default:

RSA-2K

2.39.8.7 Destination-PKCS12-File

Internal destination where the received certificate is saved.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

ssl_pkcs12_int
Certificate store for WEBconfig certificates.

Default:

ssl_pkcs12_int

2.39.8.8 Authorization-Challenges

Specifies the method used to perform the Let's Encrypt authorization challenge.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

http-01
Authorization is performed over HTTP and port 80.

tls-alpn-01
Authorization is performed over TLS and port 443.

http-01,tls-alpn-01
http-01 is preferred over tls-alpn-01.

tls-alpn-01,http-01
tls-alpn-01 is preferred over http-01.

Default:

tls-alpn-01,http-01

2.39.8.10 SSL

In this menu, you configure the settings for a SSL/TLS secured connection to the Let's Encrypt server.

Console path:

Setup > **Certificates** > **ACME-Client**

2.39.8.10.1 Versions

Here, select the encryption protocols for the TLS connection.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

2.39.8.10.2 Keyex-Algorithms

Here, select the encryption method for the SSL/TLS connection.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.39.8.10.3 Crypto-Algorithms

Here, select the crypto algorithms for the SSL/TLS connection.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

2.39.8.10.4 Hash-Algorithms

Here, select the hash algorithms for the SSL/TLS connection.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

MD5
SHA1
SHA-2-256
SHA2-384

Default:

SHA-2-256

SHA2-384

2.39.8.10.5 Prefer-PFS

Specify whether PFS (perfect forward secrecy) is enabled for the SSL/TLS secured connection.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.39.8.10.6 Renegotiations

With this setting you control whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Ignored

2.39.8.10.7 Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

x25519

x25519 is used for encryption.

x448

x448 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

x25519

x448

2.39.8.10.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
MD5-ECDSA
SHA1-ECDSA
SHA224-ECDSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default:

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA

2.39.8.10.22 Min-DH-Length

This value refers to the Diffie-Hellman agreement used to derive the master secret for the SSL tunnel, more precisely to the length range of the keys used for this purpose. Sensible lengths are in the range 2048…8192.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

Max. 4 characters from `[0-9]`

Default:

2048

2.39.8.10.23 Max-DH-Length

This value refers to the Diffie-Hellman agreement used to derive the master secret for the SSL tunnel, more precisely to the length range of the keys used for this purpose. Sensible lengths are in the range 2048…8192.

Console path:

Setup > **Certificates** > **ACME-Client** > **SSL**

Possible values:

Max. 4 characters from `[0-9]`

Default:

8192

2.39.8.11 Endpoint-Loopback-Address

Enter the loopback address for the ACME router here.

Console path:

Setup > **Certificates** > **ACME-Client**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.39.8.21 Manually-Fetch-Certificate

With this action you trigger a manual fetch of the certificate.

Console path:

Setup > **Certificates** > **ACME-Client**

2.39.8.22 Auto-Fetch-Certificate

Settings for automatically fetching and renewing the certificate.

Console path:

Setup > **Certificates** > **ACME-Client**

2.39.8.22.1 Operating

Activates or deactivates the automatic fetching and renewal of the certificate.

Console path:

Setup > **Certificates** > **ACME-Client** > **Auto-Fetch-Certificate**

Possible values:

Yes
No

Default:

No

2.39.8.22.2 Minimum-Validity-Days

Minimum number of days before expiry for the certificate to be renewed.

Console path:

Setup > **Certificates** > **ACME-Client** > **Auto-Fetch-Certificate**

Possible values:

Max. 5 characters from `[0-9]`

Default:

30

2.40 GPS

Enter the URL for the OCSP client to access the OCSP responder.

Console path:

Setup

2.40.1 Operating

Activate or deactivate the GPS function here. You can activate the GPS module independently of the location verification function, for example to monitor the current positional coordinates with LANmonitor.

Console path:

Setup > **GPS**

Possible values:

No
Yes

Default:

No

2.41 UTM

You can adjust the UTM settings here.

Console path:

Setup

2.41.2 Content-Filter

The settings for the content filter are located here.

Console path:

Setup > **UTM**

2.41.2.1 Operating

The settings for the content filter are located here.

Console path:

Setup > **UTM** > **Content-Filter**

Possible values:

No

Deactivates the content filter.

Yes

Activates the content filter.

Default:

No

2.41.2.2 Global settings

The global settings for the content filter are located here.

Console path:

Setup > **UTM** > **Content-Filter**

2.41.2.2.1 Admin-Email

An SMTP client must be defined if you wish to use the e-mail notification function. You can use the client in the device, or another client of your choice.

No e-mail will be sent if no e-mail recipient is defined,.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

2.41.2.2.5 Action-On-Error

This is where you can determine what should happen when an error occurs. For example, if the rating server cannot be contacted, this setting either allows the user to surf without restrictions or access to the web is blocked entirely.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Block
Pass

Default:

Block

2.41.2.2.6 Action on license exceedance

This is where you can determine what should happen when the licensed number of users is exceeded. Users are identified by their IP address. The system keeps count of the IP addresses that connect via the LANCOM Content Filter. When the eleventh user establishes a connection with a 10-user license, no further checking is performed by the LANCOM Content Filter. Depending on this setting, the unlicensed user can either surf the web without restrictions, or access to the web is blocked entirely.

The users of the content filter are automatically removed from the user list when no connection has been made from the IP address concerned via the content filter for 5 minutes.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Block
Pass

Default:

Block

2.41.2.2.7 Action on license expiration

The license to use the LANCOM Content Filter is valid for a certain period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires (at the e-mail address configured in LANconfig under **Log & Trace** > **General**).

This is where you can specify what should happen when the license expires (i.e. block everything or allow everything through). After the license expires, this setting either allows the user to surf the web without restrictions, or access to the web is blocked entirely.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Block
Pass

Default:

Block

2.41.2.2.9 News

This is where you define how you wish to receive notification of specific events. Notification can be made by e-mail, SNMP or SYSLOG. You can specify that messages for different events should be output in different ways.

Table 19: Notification

Event type	Source	Priority	Default
Error	System	Alert	SYSLOG notification
License exceedance	Administration	Alert	E-MAIL, SNMP and SYSLOG notification
License expiry	Administration	Alert	E-MAIL, SNMP and SYSLOG notification
Override	Router	Alert	No notification
Proxy-Limit	Router	Info	SYSLOG notification

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

2.41.2.2.9.1 Cause

Here you choose one of the predefined values for the cause for notification.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings** > **Notification**

2.41.2.2.9.2 E-mail

Here you specify whether you want to receive notifications by e-mail.

The option presettings differ depending on the cause.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings** > **Notifications**

Possible values:

Off
Immediate
Daily

2.41.2.2.9.3 SNMP

You can specify whether you want to receive notification by SNMP here.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings** > **Notification**

Possible values:

No
Yes

2.41.2.2.9.4 Syslog

You can specify whether you want to receive notification by SYSLOG here.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings** > **Notification**

Possible values:

No
Yes

2.41.2.2.10 Block-Text

This is where you can define text to be displayed when blocking occurs. Different blocking texts can be defined for different languages. The display of blocking text is controlled by the language setting transmitted by the browser (user agent).

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

2.41.2.2.10.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language. Examples of the country code:

de-DE

German-Germany

de-CH

German-Switzerland

de-AT

German-Austria

en-GB

English-Great Britain

en-US

English-United States

The content filter processes only the first part of the country code to the "-", i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code set in the browser is not

found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Block-Text**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.2.10.2 Text

Enter the text that you wish to use as blocking text for this language.

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

<CF-URL/>

For a forbidden URL

<CF-HOST/> or <CF-DOMAIN/>

Displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.

<CF-CATEGORIES/>

For the list of categories used to block the website.

<CF-PROFILE/>

For the profile name

<CF-DURATION/>

Displays the override duration in minutes.

<CF-OVERRIDEURL/>

For the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)

<CF-LINK/>

Adds a link for activating the override.

<CF-BUTTON/>

Adds a button for activating the override.

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

The following attributes are available:

BLACKLIST	If the site was blocked because it is in the profile blacklist.
FORBIDDEN	If the site was blocked due to one of its categories.
CATEGORY	If the override type is "Category" and the override was successful
ERR	If an error has occurred.

Since there are separate text tables for the blocking page and the error page, this tag only makes sense if you have configured an alternative URL to show on blocking.

OVERRIDEOK	If users have been allowed an override (in this case, the page should display an appropriate button).

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example:

<CF-URL/> is blocked because it matches the categories <CF-CA/>. Your content profile is <CF-PR/>. <CF-IF OVERRIDEOK> <CF-BU/></CF-IF>

The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Block-Text**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.2.11 URL-To-Show-On-Blocking

This is where you can enter the address of an alternative URL. If access is blocked, the URL entered here will be displayed instead of the requested web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same HTML tags here as used in the blocking text. If you do not make any entry here, the default page stored in the device will be displayed..

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.2.12 Loopback-To-Use-On-Blocking

This is where you can configure an optional sender address for the blocked URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If there is an interface called "DMZ", its address will be taken in this case.

GUEST
LBO…LBF for the 16 loopback addresses.
Any IP address in the form `x.x.x.x`.

2.41.2.2.13 Override active

This is where you can activate the override function and make further related settings.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

No
Yes

Default:

No

2.41.2.2.14 Override-Duration

The override duration can be restricted here. When the period expires, any attempt to access the same domain and/or category will be blocked again. Clicking on the override button once more allows the web site to be accessed again for the duration of the override and, depending on the settings, the administrator will be notified once more.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

1 … 1440 Minutes

Default:

5

2.41.2.2.15 Override-Type

This is where you can set the type of override. It can be allowed for the domain, for the category of web site to be blocked, or for both.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Category

For the duration of the override, all URLs are allowed that fall under the affected categories (as well as those which would already have been allowed even without the override).

Domain

For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.

Category-and-Domain

For the duration of the override, all URLs are allowed that belong to this domain and also to the allowed categories. This is the highest restriction.

Default:

Category-and-Domain

2.41.2.2.17 Save-to-Flashrom

Activate this option for the category statistics to be stored to the flash ROM.

This ensures that the data is not lost even if the device is switched off or suffers a power outage.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Yes

Activates storage to the flash ROM.

No

Deactivates storage to the flash ROM.

Default:

No

2.41.2.2.19 Error text

This is where you can define text to be displayed when an error occurs.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Yes

Activates storage to the flash ROM.

No

Deactivates storage to the flash ROM.

Default:

No

2.41.2.2.19.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language. Examples of the country code:

The content filter processes only the first part of the country code to the "-", i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

de-DE

German-Germany

de-CH

German-Switzerland

de-AT

German-Austria

en-GB

English-Great Britain

en-US

English-United States

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Error-Text**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.2.19.2 Text

Enter the text that you wish to use as error text for this language.

You can also use HTML tags for the error text. The following empty element tags can be used as tag values:

<CF-URL/>	For a forbidden URL.

<CF-HOST/> or <CF-DOMAIN/>	Displays the host or the domain for the blocked URL. The tags are of equal value and their use is optional.
<CF-DURATION/>	Displays the override duration in minutes.
<CF-PROFILE/>	For the profile name.
<CF-ERROR/>	For the error message.

You can use a tag with attributes to display or hide parts of the HTML document: `<CF-IF att1 att2> ... </CF-IF>`.

Possible attributes are:

CHECKERROR	The error occurred while checking the URL.
OVERRIDEERROR	The error occurred while approving an override.

Example

<CF-URL/> is blocked because an error occurred	 <CF-ERROR/>

<CF-URL>: Blocked URL <CF-HOST> or <CF-DOMAIN>: Host part of the blocked URL <CF-PROFILE>: User content-filter profile <CF-DURATION>: Override time in minutes <CF-ERROR>: Error message <CF-IF> to </CF-IF>: Conditional evaluation of the following parameters with the logical OR: CHECKERROR: The error occurred while checking the URL (as earlier) OVERRIDE ERROR: The error occurred while approving an override

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Error-Text**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

<CF-IF CHECK><CF-URL/> is blocked</CF-IF><CF-IF OVERRIDE>The override failed</CF-IF> due to the following error:

<CF-ERROR/>

2.41.2.2.20 Override text

This is where you can define text that is displayed to users confirming an override.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

2.41.2.2.20.1 Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language. Examples of the country code:

The content filter processes only the first part of the country code to the "-", i.e. "en", "en-GB" and "en-US" are identical to the content filter. The content filter is not case-sensitive. If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

de-DE

German-Germany

de-CH

German-Switzerland

de-AT

German-Austria

en-GB

English-Great Britain

en-US

English-United States

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Override-Text**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.41.2.2.20.2 Text

You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

Enter the text that you wish to use as override text for this language. The following tags can be used as tag values:

<CF-URL/>	For the originally forbidden URL that is now allowed.
<CF-CATEGORIES/>	For the list of categories that have now been allowed as a result of the override (except if domain override is specified).
<CF-BUTTON/>	Displays an override button that forwards the browser to the original URL.
<CF-LINK/>	Displays an override link that forwards the browser to the original URL.
<CF-HOST/> or <CF-DOMAIN/>	Displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.

You can use a tag with attributes to display or hide parts of the HTML document: `<CF-IF att1 att2> ... </CF-IF>`.

Possible attributes are:

CHECKERROR	The error occurred while checking the URL.
OVERRIDEERROR	The error occurred while approving an override.

<CF-ERROR/>	Generates an error message in the event that the override fails.
<CF-DURATION/>	Displays the override duration in minutes.

You can use a tag with attributes to display or hide parts of the HTML document: <CF-IF att1 att2> ... </CF-IF>.

Attributes can be:

BLACKLIST	If the site was blocked because it is in the profile blacklist.
FORBIDDEN	If the site was blocked due to one of its categories.
CATEGORY	If the override type is "Category" and the override was successful.
DOMAIN	If the override type is "Domain" and the override was successful.
BOTH	If the override type is "Category-and-Domain" and the override was successful.
ERROR	If the override fails.
OK	If either CATEGORY or DOMAIN or BOTH are applicable.

If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

Example

<CF-IF CA BO>The categories <CF-CAT/> are</CF-IF><CF-IF BO> in the domain <CF-DO/></CF-IF><CF-IF DO>The domain <CF-DO/> is</CF-IF><CF-IF OK> released for <CF-DU/> minutes. <CF-LI/></CF-IF><CF-IF ERR>Override error: <CF-ERR/></CF-IF>

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Override-Text**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.2.23 Snapshot

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to "0".

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

2.41.2.2.23.1 Active

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to "0".

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Snapshot**

Possible values:

No

Deactivates the snapshot.

Yes

Activates the snapshot.

Default:

Yes

2.41.2.2.23.2 Type

Here you decide whether the snapshot should be taken monthly, weekly or daily.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Snapshot**

Possible values:

Monthly
Weekly
Daily

Default:

Weekly

2.41.2.2.23.3 Time

If you require a daily snapshot, then enter here the time of day for the snapshot in the format HH:MM.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Snapshot**

Possible values:

Max. 5 characters from `[0-9]:`

Default:

00:00>

2.41.2.2.23.4 Day

For monthly snapshots, set the day of the month when the snapshot should be taken.

It is advisable to select a number between 1 and 28 in order to ensure that it occurs every month.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Snapshot**

Possible values:

Max. 2 characters from `[0-9]`

Default:

1

2.41.2.2.23.5 Day of week

For weekly snapshots, set the day of the week when the snapshot should be taken.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings** > **Snapshot**

Possible values:

Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

Default:

Sunday

2.41.2.2.24 Proxy-Connections-Limit

This setting is for the maximum allowable number of simultaneous proxy connections. This limits the load that can be placed on the system. A notification is sent if this number should be exceeded.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

0 … 999999

Default:

Depends on device

2.41.2.2.25 Processing-Timeout-in-ms

Specifies the maximum time in milliseconds that the proxy can take for processing. A timeout error page is displayed if this time is exceeded.

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

0 … 999999 Milliseconds

Default:

3000

Special values:

0

The value "0" sets no time limit.

Values less than 100 milliseconds make no sense.

2.41.2.2.21 URL to show on error

This is where you can enter an alternative URL. In the event of an error, the URL entered here will be displayed instead of the usual web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the override text. If you do not make any entry here, the default page stored in the device will be displayed..

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

Possible values:

- Valid URL address

Default: Blank

2.41.2.2.22 Loopback to use on error

This is where you can configure an optional sender address for the error URL to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

Telnet path: /Setup/UTM/Content-Filter/Global-Settings

English description: Loopback-To-Use-On-Override

Possible values:

- Name of the IP networks whose address should be used
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0…LBF for the 16 loopback addresses
- GUEST
- Any IP address in the form x.x.x.x

Default: Blank

The sender address specified here is used unmasked for every remote station.

2.41.2.2.28 Loopback-To-Rating-Server

This setting gives you the option to specify the loopback address used by the device to connect to the rating server. If you have configured loopback addresses, you can specify them here as sender address.

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

Name of the IP network (ARF network), whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If an interface with the name "DMZ" already exists, the device will select that address instead.

LBO…LBF for the 16 loopback addresses.
GUEST
Any IP address in the form `x.x.x.x`.

2.41.2.2.29 Wildcard

With this feature enabled, Web sites with wildcard certificates (consisting of CN entries such as `*.mydomain.com`) are verified using the main domain (`mydomain.com`). Verification is evaluated in this sequence:

- Server name check in the "Client Hello" (depends on the browser used)
- Check of the CN in the SSL certificate that you received
- Entries with wildcards are ignored
- If the CN cannot be verified, the field "Alternative Name"is evaluated.
- DNS reverse lookup of the associated IP address and verification of the host name obtained
- If wildcards are included in the certificate, the main domain is checked instead (corresponds to the above function)
- Verification of the IP address

Console path:

Setup > **UTM** > **Content Filter** > **Global settings**

Possible values:

No
Yes

Default:

No

2.41.2.2.30 Unknown 443 traffic

Here, you can permit non-HTTPS communication via TCP port 443.

Console path:

Setup > **UTM** > **Content-Filter** > **Global-Settings**

Possible values:

0

Deny

1

Allow

Default:

0

2.41.2.3 Profiles

The profile settings for the content filter are located here.

Console path:

Setup > **UTM** > **Content-Filter**

2.41.2.3.1 Profiles

This is where you can create content filter profiles that are used to check web sites for prohibited content. A content-filter profile always has a name and, for various time periods, it activates the desired category profile and, optionally, a blacklist and a whitelist.

In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content-filter profile is thus made up of the sum of all entries with the same name.

The firewall refers to this content-filter profile.

Please note that you must make corresponding settings in the firewall in order to use the profiles in the Content Filter.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles**

2.41.2.3.1.1 Name

Enter the name of the content filter profile to be used for referencing in the firewall.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.41.2.3.1.2 Timeframe

Select the timeframe for the content filter profile. The timeframes “ALWAYS” and “NEVER” are predefined. Further time frames can be configured under:**Setup** > **Time** > **Timeframe**

A content-filter profile may have several lines with different timeframes.

If timeframes overlap when multiple entries are used for a content filter profile, all pages contained in one of the active entries will be blocked for that period of time. If multiple entries are used for a content-filter profile and a time period remains undefined, access to all web sites will be unchecked for this period.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Profiles**

Possible values:

Always
Never
Name of a timeframe profile

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.41.2.3.1.3 Whitelist

Select the whitelist that applies to this content filtering profile. Enter a new name or select an existing entry from the whitelist table.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.41.2.3.1.4 Blacklist

Select the blacklist that applies to this content filtering profile. Enter a new name or select an existing entry from the blacklist table.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.3.1.5 Category profile

Select the category profile that applies to this content filtering profile. Enter a new name or select an existing entry from the table of category profiles.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.3.2 Whitelists

This is where you can configure web sites to which access is to be allowed.

Entries for the allowed web sites may contain up to 252 characters. To define longer whitelist entries, a number of entries can use a special, shared name. Enter the name of the whitelist followed by a # character and any suffix. For example, you create three whitelist entries called "MyWhitelist#1", "MyWhitelist#2" and "MyWhitelist#3". In the content filtering profile, you can reference this extended whitelist with the name "MyWhitelist".

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles**

2.41.2.3.2.1 Name

Enter the name of the whitelist for referencing from the content-filter profile.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Whitelist**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.41.2.3.2.2 Whitelist

This is where you can configure web sites which are to be checked locally and then accepted.

The following wildcard characters may be used:

*****

For any combination of more than one character (e.g. www.example.* encompasses the web sites www.example.de, www.example.eu, www.example.es, etc.)

?

For any one character (e.g. www.example.e* encompasses the web sites www.example.eu, www.example.es)

URLs must be entered without the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/ . For this reason it is advisable to enter the URL as: www.mycompany.de*.

Individual URLs are separated by a blank.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Whitelist**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.41.2.3.3 Blacklists

This is where you can configure those web sites that are to be blocked.

Entries for the forbidden web sites may contain up to 252 characters. To define longer blacklist entries, a number of entries can use a special, shared name. Enter the name of the blacklist followed by a # character and any suffix. For example, you create three blacklist entries called "MyBlacklist#1", "MyBlacklist#2" and "MyBlacklist#3". In the content filtering profile, you can reference this extended blacklist with the name "MyBlacklist".

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles**

2.41.2.3.3.1 Name

Enter the name of the blacklist for referencing from the content-filter profile.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Blacklist**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.41.2.3.3.2 Blacklist

Access to the URLs entered here will be forbidden by the blacklist.

The following wildcard characters may be used:

*****

For any combination of more than one character (e.g. www.example.* encompasses the web sites www.example.de, www.example.eu, www.example.es, etc.)

?

For any one character (e.g. www.example.e* encompasses the web sites www.example.eu, www.example.es)

URLs must be entered without the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. www.mycompany.de/ . For this reason it is advisable to enter the URL as: www.mycompany.de*.

Individual URLs are separated by a blank.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Blacklist**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.41.2.3.4 Category profiles

Here you create a category profile and determine which categories or groups should be used to rate web sites for each category profile. You can allow or forbid the individual categories or activate the override function for each group.

Supported devices are LANCOM devices with an activated Content Filter option

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles**

2.41.2.3.4.1 Name

The name of the category profile for referencing from the content-filter profile is entered here.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.41.2.3.4.100 Name

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.101 Pornography

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.102 Erotic/Sex

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.103 Swimwear/Lingerie

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.104 Shopping

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.105 Auctions/Classified_Ads

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.106 Governmental/Non-Profit_Organizations

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.107 Non-Governmental_Organizations

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

2.41.2.3.4.108 Cities/Regions/Countries

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.109 Education

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.110 Political_Parties

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.111 Religion/Spirituality

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.112 Sects

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.113 Illegal_Activities

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.114 Computer_Crime/Warez/Hacking

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.115 Political_Extreme/Hate/Discrimination

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.116 Warez/Software_Privacy

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.117 Violence/Extreme

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.118 Gambling/Lottery

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.119 Computer_Games

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.120 Toys

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.121 Cinema/Television/Social_Media

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.122 Recreational_Facilities/Theme_Parks

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.123 Arts/Museums/Theaters

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.124 Music/Radio_Broadcast

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.125 Literature/Books

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.126 Humor/Cartoons

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.127 News/Magazines

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.128 Webmail/Unified_Messaging

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.129 Chat

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.130 Blogs/Bulletin_Boards

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.131 Mobile_Telephony

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.132 Digital_Postcards

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.133 Search_Engines/Web_Catalogs/Portals

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.134 Software/Hardware

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.135 Communication_Services

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.136 IT_Security/IT_Information

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.137 Web_Site_Translation

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.138 Anonymous_Proxies

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.139 Illegal_Drugs

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.139 Alcohol/Tobacco

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.141 Tobacco

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.142 Self_Help/Addiction

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.143 Dating/Networks

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.144 Restaurants/Entertainment_Venues

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.145 Travel

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.146 Fashion/Cosmetics/Jewelry

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.147 Sports

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.148 Architecture/Construction/Furniture

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.149 Environment/Climate/Pets

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.150 Personal_Web_Sites

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.151 Job_Search

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.152 Finance/Investment

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.153 Financial_Services/Insurance/Real_Estate

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.150 Banking

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.155 Vehicles

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.156 Weapons/Military

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.157 Medicine/Health/Self-Help

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.158 Abortion

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.160 Spam_URLs

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.161 Malware

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.162 Phishing_URLs

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.163 Instant_Messaging

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.167 General_Business

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.174 Banner_Advertisements

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.177 Social_Networking

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.178 Business_Networking

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.179 Social_Media

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.180 Web_Storage

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.181 Command/Control_Server

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.182 Botnet_Command_and_Control_Server

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.183 Cloud

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.184 Infrastructure_as_a_service

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.185 Platform_as_a_service

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.41.2.3.4.186 Software_as_a_service

For each main category or the associated sub-categories, you define whether the URLs are to be allowed, forbidden or allowed with override only.

To enable the category profile, assign it to a Content Filter profile along with a time frame.

Console path:

Setup > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Possible values:

Allowed
Forbidden
Override

Default:

Allowed

2.42 xDSL

The Asymmetrical Digital Subscriber Line (ADSL) and Very High Speed Digital Subscriber Line (VDSL) are transmission methods for high-speed data transmissions over regular telephone lines.

With ADSL and ADSL2+, transmissions (downstream) of up to 24 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 3.5 Mbps (upstream) - hence the name "asymmetric". As an example, the ADSL-over-ISDN infrastructure operated in Germany supports maximum speeds of 16 Mbps (downstream) and 1125 kbps (upstream).

VDSL is a DSL technology that delivers far higher data rates over normal phone lines than, for example, ADSL or ADSL2+.

Console path:

Setup

2.42.3 WAN-Bridge

Here you configure the router for ADSL/VDSL modem operation (bridge mode).

Console path:

Setup > **xDSL**

2.42.3.1 Interface

The xDSL interfaces of the device.

Console path:

Setup > **xDSL** > **WAN-Bridge**

2.42.3.2 Mode

The device is able to work in bridge mode. It then behaves like an ADSL/VDSL modem.

Console path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Router

The device works as a router.

Bridge

The device works in bridge mode.

Default:

Router

2.42.3.3 ATM-VPI

Virtual Path Identifier (VPI). The value for VPI is communicated by the ADSL/VDSL network operator. The default value is for Deutsche Telekom.

Console path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

2.42.3.4 ATM-VCI

Virtual Channel Identifier (VCI). The value for VCI is communicated by the ADSL/VDSL network operator. The default value is for Deutsche Telekom.

Console path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Max. 5 characters from `[0-9]`

Default:

32

2.42.3.5 ATM-Muxmode

This setting sets the encapsulation method used for the data packets. The default value is for Deutsche Telekom.

Console path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

VC-MUX

Multiplexing via ATM by establishing additional VCs as per RFC 2684.

LLC-MUX

Multiplexing via ATM with LLC/SNAP encapsulation as per RFC 2684. Several protocols can be transmitted over the same VC (virtual channel).

Default:

LLC-MUX

2.42.5 General

This table contains the settings for the modem firmware. As there is no “best” DSL firmware for every situation, you can switch to another modem firmware available in the LCOS, if necessary.

Console path:

Setup > **xDSL**

2.42.5.1 Interface

Fixed value for this interface: 1 for XDSL-1, 2 for XDSL-2, etc.

Console path:

Setup > **xDSL** > **General**

2.42.5.2 Vendor-ID

The code specified by the German Federal Network Agency for LANCOM devices does not work in all countries. In these cases, for example in Switzerland, the alternative identifier must be selected.

Console path:

Setup > **xDSL** > **General**

Possible values:

Default-ID
Alternate-ID

Default:

Default-ID

2.42.5.3 Sync-limits-Tx-Rate

This setting makes it possible to deactivate the limitation of the transmission data rate to the sync data rate. This is used for quality assurance tests, for example to determine the data rate at which the modem puts a limit on throughput.

Console path:

Setup > **xDSL** > **General**

Possible values:

On

The sync data rate is used as the QoS data rate.

Off

The sync data rate is not used and the interface behaves like a DSL interface with regard to the QoS data rate.

Default:

On

2.42.5.4 Modem-Firmware

This switch allows you to swap between two versions of the modem firmware stored in the LCOS.

This column is only available for devices with a LCOS that contains an alternative modem firmware.

Console path:

Setup > **xDSL** > **General**

Possible values:

Default

This chooses the version preferred by LANCOM.

Alternate

This setting selects a version that improves the behavior at some connections.

Default:

Default

2.44 CWMP

The CPE WAN Management Protocol (CWMP) enables devices to be remotely configured via a WAN link. Communication between the device (customer premises equipment, CPE) and the configuration server (auto configuration server, ACS) is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC).

Console path:

Setup

2.44.2 Operating

Enables or disables CWMP.

Console path:

Setup > **CWMP**

Possible values:

No
Yes

Default:

No

2.44.3 Allow file download

This switch allows you to transfer a firmware or a script file from the ACS (auto configuration server) to this device.

Console path:

Setup > **CWMP**

Possible values:

No
Yes

Default:

No

2.44.4 Inform retry limit

Here you specify how many times the CPE attempts to deliver an inform message to the ACS after a failure.

Console path:

Setup > **CWMP**

Possible values:

Max. 10 characters from `0123456789`

Default:

10

Special values:

0

Retry disabled

2.44.5 Source address

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address. If you have configured loopback addresses, you can specify them here as source address.

If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

Console path:

Setup > **CWMP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Special values:

Name of the IP network (ARF network), whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", then the device takes its address).
LB0…LBF for one of the 16 loopback addresses or its name
Any IP address in the form x.x.x.x.

Default:

empty

2.44.6 ACS URL

Here you enter the address of the ACS (auto configuration server) which the device connects to. The address is entered in the IPv4, IPv6, or FQDN format.

Console path:

Setup > **CWMP**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.7 ACS username

Enter a user name for the device to use when connecting with the ACS (auto configuration server).

Console path:

Setup > **CWMP**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.8 ACS password

Enter a password for the device to use when connecting with the ACS (auto configuration server).

Console path:

Setup > **CWMP**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.9 Periodic inform activated

Enables or disables the sending of periodic inform messages from the device to the ACS (auto configuration server).

Console path:

Setup > **CWMP**

Possible values:

No
Yes

Default:

No

2.44.10 Periodic inform interval

This is the interval in seconds between two periodic inform messages sent by the device to the ACS (auto configuration server). The ACS then requests further information from the device.

The default value is 1200 seconds (20 minutes). Do not set a value that is too small, as inform messages increase network load. The interval does not commence before the device and server have exchanged all of the necessary information.

Console path:

Setup > **CWMP**

Possible values:

Max. 10 characters from `0123456789`

Default:

1200

Special values:

0

Periodic-Inform disabled

2.44.11 Periodic inform time

Specify the periodic inform time. This entry in the “dateTime” format contains the time for the first inform message. Example: `0001-02-03T03:04:05+06:00`.

Console path:

Setup > **CWMP**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.12 Connection request username

Select one of the configured device administrators to be used by the ACS (auto configuration server) when connecting to this device. The name you select must be an enabled device administrator with appropriate privileges, i.e. root access to change the firmware.

Console path:

Setup > **CWMP**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.13 Updates managed

This switch allows the ACS (auto configuration server) to make firmware modifications to the device.

Console path:

Setup > **CWMP**

Possible values:

No
Yes

Default:

No

2.44.14 Allow user change

This switch allows the ACS (auto configuration server) to change the device administrator or to change the name of the device administrator that it uses to connect to the device.

Console path:

Setup > **CWMP**

Possible values:

No
Yes

Default:

No

2.44.18 Data-model

Use this entry to specify the CWMP data model.

Console path:

Setup > **CWMP**

Possible values:

TR-098
TR-181

Default:

TR-181

2.44.19 Local port

Sets the local port for CWMP.

Console path:

Setup > **CWMP**

Possible values:

Max. 5 characters from `[0-9]`

Default:

7547

2.44.20 Connection request password

For the configured device administrator, set a password to be used by the ACS (auto configuration server) when connecting to this device.

Repeat the password in the next field.

Console path:

Setup > **CWMP**

Possible values:

Max. 256 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.44.23 Configuration managed

Enable or disable the management of the CWMP configuration.

Console path:

Setup > **CWMP**

Possible values:

No

Management of the configuration is disabled.

Yes

Management of the configuration is enabled.

Default:

Yes

2.44.26 SSL

This menu contains the encryption parameters for the CWMP.

Console path:

Setup > **CWMP**

2.44.26.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.44.26.2 Key-exchange algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.44.26.3 Crypto-Algorithms

This entry specifies which cryptographic algorithms are allowed.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.44.26.4 Hash algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.44.26.5 Prefer PFS

This option means that your device always prefers to connect with PFS (Perfect Forward Secrecy), regardless of the default setting of the client.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.44.26.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.
Allowed
The device permits renegotiations with the remote station.
Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.44.26.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1

secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.44.26.21 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **CWMP** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.44.28 Blocked-Peers

The TR069 server cannot usually be reached via every Internet connection (e.g. backup connections). Communication with the server may also not be useful if, for example, the client cannot be identified by the server via this communication channel.

For this reason, comma-separated remote stations can be entered here via which no contact with the TR069 server may be established.

Console path:

Setup > **CWMP**

Possible values:

Max. 256 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.45 SLA monitor

This menu contains the settings for the SLA monitor.

Console path:

Setup

2.45.1 ICMP

This menu is used to configure the Internet Control Message Protocol (ICMP).

Console path:

Setup > **SLA-Monitor**

2.45.1.1 Name

Contains the name of the ICMP configuration.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.45.1.2 Active

This entry controls whether the ICMP profile is actually used.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Yes
No

Default:

Yes

2.45.1.3 Destination

Set an IPv4 address to which the ICMP sends diagnostic and error messages.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 40 characters from `[0-9].`

Default:

0.0.0.0

2.45.1.4 Rtg-Tag

Enter the routing tag for setting the route to the relevant remote gateway.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.45.1.5 Loopback address

The device sees this address as its own address, which is also available even if a physical interface is disabled, for example.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 56 characters from `[0-9]`

Default:

empty

2.45.1.6 Interval

The interval in seconds in which the ICMP sends diagnostic or error messages to the specified destination.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 6 characters from `[0-9]`

Default:

30

2.45.1.7 Start offset

Here you specify a startup delay for the ICMP transmissions in milliseconds.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

2.45.1.8 Count

Set the number of ICMP packets to be transmitted at the same time.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

5

2.45.1.9 Packet delay

Sets delay before the ICMP packets are transmitted. Delay in milliseconds.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

1000

2.45.1.10 Packet size

Sets the packet size for ICMP messages. The value is set in bytes.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 5 characters from `[0-9]`

Default:

56

2.45.1.11 Warn-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor emits a warning.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

100

2.45.1.12 Crit-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor reports an error.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

200

2.45.1.13 Warn-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor emits a warning.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0–9]`

Default:

80

2.45.1.14 Crit-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor reports an error.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0–9]`

Default:

170

2.45.1.15 Warn-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before a warning is issued.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0–9]`

Default:

10

2.45.1.16 Crit-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before an error message is issued.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

20

2.45.1.17 IP-Version

Specifies the IP standard used for the Internet Control Message Protocol.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Auto
IPv4
IPv6

Default:

Auto

2.45.1.19 Comment

Comment about this ICMP configuration.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.45.1.20 Warn-Lvl-Jitter

Runtime variance of data packets (jitter) in milliseconds before a warning is issued.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

80

2.45.1.21 Crit-Lvl-Jitter

Runtime variance of data packets (jitter) in milliseconds before an error message is issued.

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

40

2.45.1.22 DSCP

Specifies the DSCP value of the ICMP message. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Console path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

BE/CS0
CS1
CS2
CS3
CS4
CS5
CS6
CS7
AF11
AF12
AF13
AF21
AF22
AF23
AF31
AF32
AF33
AF41
AF42
AF43
EF

2.45.2 Event count

Number of events to be logged by the SLA monitor.

Console path:

Setup > **SLA-Monitor**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

2.45.3 Startup delay

Delay time in milliseconds before monitoring is started.

Console path:

Setup > **SLA-Monitor**

Possible values:

Max. 3 characters from `[0-9]`

Default:

10

2.52 COM-Ports

The trace mode determines whether values issued by the ADSL trace also include internal status values (extended) or the line status (simple) only.

Console path:

Setup

2.52.1 Devices

The serial interfaces in the device can be used for various applications, for example for the COM port server or as a WAN interface. The Devices table allows individual serial devices to be assigned to certain applications.

Console path:

Setup > **COM-Ports**

2.52.1.1 Device type

Selects a serial interface from the list of those available in the device.

Console path:

Setup > **COM-Ports** > **Devices**

2.52.1.4 Service

Activation of the port in the COM port server.

Console path:

Setup > **COM-Ports** > **Devices**

Possible values:

WAN
COM-port server
UPS
ePaper

Default:

WAN

2.52.2 COM-port server

This menu contains the configuration of the COM-port server.

Console path:

Setup > **COM-Ports**

2.52.2.1 Operation

This table activates the COM port server at a port of a certain serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to stop the corresponding server instance.

Console path:

Setup > **COM-Ports** > **COM-Port-Server**

2.52.2.1.1 Device type

Selects a serial interface from the list of those available in the device.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Operational**

2.52.2.1.2 Port number

Some serial devices such as the CardBus have more that one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Operational**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

For serial interfaces with just one port, e.g. outband.

2.52.2.1.4 Operating

Activates the COM port server on the selected port of the selected interface.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Operational**

Possible values:

No
Yes

Default:

No

2.52.2.2 COM-Port-Settings

This table contains the settings for data transmission over the serial interface.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.

Console path:

Setup > **COM-Ports** > **COM-Port-Server**

2.52.2.2.1 Device type

Selects a serial interface from the list of those available in the device.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

2.52.2.2.2 Port number

Some serial devices such as the CardBus have more that one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

For serial interfaces with just one port, e.g. outband.

2.52.2.2.4 Bitrate

Bitrate used on the COM port

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

110 … 230400

Default:

9600

2.52.2.2.5 Data bits

Number of data bits.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

7
8

Default:

8

2.52.2.2.6 Parity

The checking method used on the COM port.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

None
Even
Odd

Default:

None

2.52.2.2.7 Stop bits

Number of stop bits.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

1
2

Default:

1

2.52.2.2.8 Handshake

The data-flow control used on the COM port.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

none
RTS/CTS

Default:

RTS/CTS

2.52.2.2.9 Ready condition

The ready condition is an important property of any serial port. The COM port server transmits no data between the serial port and the network if the status is not "ready". Apart from that, in the client mode the act of switching between the "ready" and "not-ready" states is used to establish and terminate TCP connections. The readiness of the port can be checked in two different ways. In DTR mode (default) only the DTR handshake is monitored. The serial interface is considered to be ready for as long as the DTR line is active. In data mode, the serial interface is considered to be active for as long as it receives data. If no data is received during the timeout period, the port reverts to its "not ready" state.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

DTR
Data

Default:

DTR

2.52.2.2.10 Ready-Data-Timeout

The timeout switches the port back to the not-ready status if no data is received. This function is deactivated when timeout is set to zero. In this case the port is always ready if the data mode is selected.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

Switches the Ready-data-timeout off.

2.52.2.3 Network settings

This table contains all settings that define the behavior of the COM port in the network.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.

Console path:

Setup > **COM-Ports** > **COM-Port-Server**

2.52.2.3 Device type

Selects a serial interface from the list of those available in the device.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

2.52.2.3.2 Port number

Some serial devices such as the CardBus have more that one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

For serial interfaces with just one port, e.g. outband.

2.52.2.3.4 TCP-Mode

Each instance of the COM port server in server mode monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused. In client mode, the instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable. In both cases the device closes any open connections when the device is restarted.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Server
Client

Default:

Server

2.52.2.3.5 Listen port

The TCP port where the COM port in TCP server mode expects incoming connections.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.52.2.3.6 Connect-Hostname

The COM port in TCP client mode establishes a connection to this host as soon as the port is in the "Ready" state.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.52.2.3.7 Connect port

The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in the "Ready" state.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.52.2.3.8 Loopback-Addr.

The COM port can be reached at this address. This is its own IP address that is taken as the source address when establishing connections. This is used to define the IP route to be used for the connection.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.52.2.3.9 RFC2217-Extensions

The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the device uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extensions with incompatible remote sites is not critical. Unexpected characters may be displayed at the remote site. A side effect of using the FRC2217 extensions may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

No
Yes

Default:

No

2.52.2.3.10 Newline conversion

Here you select the character to be output by the serial port when binary mode is activated.

This setting is independent of the application communicating via the serial port. If the port is connected to another device, you can either enter CRLF here or just CR. This is because the outband interface of these devices expects a "carriage return" for the automatic determination of data-transfer speed. However, some Unix applications interpret CRLF as a prohibited double line feed character. In these cases enter either CR or LF.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

CRLF
CR
LF

Default:

CRLF

2.52.2.3.12 TCP-Retry-Timeout

Maximum time for the retransmission timeout. This timeout defines the the interval between checking TCP-connection status and reporting the result to the application using the TCP connection.

The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

0 … 99 Seconds

Default:

0

Special values:

0

Uses the RFC 1122 default value (60 seconds).

2.52.2.3.13 TCP-Retry-Count

The maximum number of attempts for checking TCP-connection status and reporting the result to the application using the TCP connection.

The maximum duration of the TCP-connection check is the product of TCP-retransmit-count and TCP-retry-count. The TCP application is only informed after the timeout for all attempts has expired. With the default values of 60 seconds timeout and max. 5 attempts, it can take up to 300 seconds before the application is informed about an inactive TCP connection.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

0 … 9

Default:

0

Special values:

0

Uses the RFC 1122 default value (5 attempts).

2.52.2.3.14 TCP-Keepalive

The RFC 1122 sets down a method of checking the availability of TCP connections, called TCP keepalive. An inactive transmitter queries the receive status from the remote station. If the TCP session to the remote site is available, then the remote responds with its receive status. If the TCP session to the remote site is not available, then the query is repeated for as long as it takes for the remote to respond with its receive status (after which a longer interval comes into play). As long as the basic connection functions, but the TCP session to the remote station is not available, then the remote station sends an RST packet which triggers the establishment of the TCP session by the requesting application.

The setting "**active**" is recommended for server applications.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Inactive

TCP keepalive is not used.

Active

TCP keepalive is active; only RST packets cause the disconnection of TCP sessions.

Proactive

TCP keepalive is active, but the request for the receive status from the remote site is only repeated for the number of times defined under "TCP retry count". If this number of requests expires without a response with the receive status, then the TCP sessions is classified as "not available" and the application is informed. If an RST packet is received during the wait time, the TCP session will be disconnected prematurely.

Default:

Inactive

2.52.2.3.15 TCP-Keepalive-Interval

This value defines the interval between sending requests for receive status if the first request is not affirmed. The associated timeout is defined as being interval/3 (max. 75 sec.).

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

Uses the RFC 1122 default values (interval 7200 seconds, timeout 75 seconds).

2.52.2.3.16 Binary mode

Using this setting you specify whether the device forwards serial data in binary format and therefore without CR/LF adjustment (CR/LF = carriage return/line feed). Since binary mode can cause problems with some serial remote stations, you should maintain the default **Auto**.

Console path:

Setup > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Possible values:

Auto

For data transmission, the COM-port server initially switches to ASCII mode; however, it uses telnet options to negotiate with the remote station whether it can switch to binary mode.

Yes

For data transmission, the COM port server switches to binary mode and does not use the telnet options to negotiate this with the remote station.

No

For data transmission, the COM port server switches to ASCII mode and does not use the telnet options to negotiate this with the remote station.

Default:

Auto

2.52.3 WAN

This menu contains the configuration of the Wide Area Network (WAN).

Console path:

Setup > **COM-Ports**

2.52.3.1 Devices

The table with WAN devices is a status table only. All Hotplug devices (connected via USB or CardBus) are automatically entered into this table.

Console path:

Setup > **COM-Ports** > **WAN**

2.52.3.1.1 Device type

List of serial interfaces available in the device.

Console path:

Setup > **COM-Ports** > **WAN** > **Devices**

2.52.3.1.3 Operating

Status of connected device.

Console path:

Setup > **COM-Ports** > **WAN** > **Devices**

Possible values:

No
Yes

Default:

No

2.53 Temperature-Monitor

The settings for the temperature monitor are located here.

Console path:

Setup

2.53.1 Upper-Limit-Degrees

When the temperature set here is exceeded, the device sends an SNMP trap of the type "trpTempMonOverTemp".

Console path:

Setup > **Temperature-Monitor**

Possible values:

0 … 127 ° Celsius

Default:

70

2.53.2 Lower-Limit-Degrees

When the temperature drops below that set here, the device sends an SNMP trap of the type "trpTempMonUnderTemp".

Console path:

Setup > **Temperature-Monitor**

Possible values:

0 … 127 ° Celsius

Default:

0

2.54 TACACS+

This menu contains the configuration settings for TACACS+.

Console path:

Setup

2.54.2 Authorization

Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

TACACS+ authorization will only activate if the defined TACACS+ server is available. If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

Console path:

Setup > **Tacacs+**

Possible values:

Disabled
Activated

Default:

Disabled

2.54.3 Accounting

Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

TACACS+ accounting will only activate if the defined TACACS+ server is available.

Console path:

Setup > **Tacacs+**

Possible values:

Disabled
Activated

Default:

Disabled

2.54.6 Shared Secret

The password for encrypting the communications between NAS and TACACS+ servers.

The password must be entered identically into the device and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

Console path:

Setup > **Tacacs+**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.54.7 Encryption

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

Console path:

Setup > **Tacacs+**

Possible values:

Disabled
Activated

Default:

Activated

2.54.9 Server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

This menu contains the settings for TACACS servers.

Console path:

Setup > **Tacacs+**

2.54.9.1 Server-address

DNS name, or IPv4 or IPv6 address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Console path:

Setup > **Tacacs+** > **Server**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.54.9.2 Loopback address

Optionally you can configure a loopback address here.

Console path:

Setup > **Tacacs+** > **Server**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.
LBO…LBF for the 16 loopback addresses.
Any IP address in the form `x.x.x.x`.

2.54.9.3 Compatibility mode

TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

Console path:

Setup > **Tacacs+** > **Server**

Possible values:

Disabled
Activated

Default:

Disabled

2.54.10 Fallback to local users

Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the device. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

The fallback to local user accounts presents a security risk if no root password is set for the device. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

Console path:

Setup > **Tacacs+**

Possible values:

Allowed
Forbidden

Default:

Allowed

2.54.11 SNMP-GET-Requests-Authorisation

This parameter allows the regulation of the behavior of devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Console path:

Setup > **Tacacs+**

Possible values:

only_for_SETUP_tree

With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

all

With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.

None

With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default:

only_for_SETUP_tree

2.54.12 SNMP-GET-Requests-Accounting

Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

This parameter allows the regulation of the behavior of devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Entering a read-only community under **Setup** > **SNMP** also enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Console path:

Setup > **Tacacs+**

Possible values:

only_for_SETUP_tree

With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.

all

With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.

None

With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

Default:

only_for_SETUP_tree

2.54.13 Bypass-Tacacs-for-CRON-scripts-action-table

You can activate or deactivate the bypassing of TACACS+ authorization and TACACS+ accounting for various actions.

Please observe that this option influences the TACACS+ function for the entire system. Be sure that you restrict the use of CRON, the action tables, and scripts only to an absolutely trustworthy circle of administrators!

Console path:

Setup > **Tacacs+**

Possible values:

Disabled
Activated

Default:

Disabled

2.54.14 Include-value-into-authorisation-request

This parameter determines, if the device only checks the CLI command or also the entered values during the authorization.

Console path:

Setup > **Tacacs+**

Possible values:

activated

If you activate this function, the device checks, if the user has permission to change certain values.

disabled

If you deactivate this function, the device only checks, if the user has permission to use a certain CLI command.

Default:

activated

2.54.15 Authorisation-Type

Defines the authorization types.

Console path:

Setup > **Tacacs+**

Possible values:

Commands

Each CLI command is authorized separately by the TACACS+ server.

Shell

Overall access to the shell (CLI) is authorized once.

Default:

Commands

2.56 Autoload

This menu is used to configure the automatic uploading of firmware or configurations from external data media.

Console path:

Setup

2.56.1 Firmware-and-Loader

This option activates the automatic loading of loader and/or firmware files from a connected USB medium.

This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

Console path:

Setup > **Autoload**

Possible values:

Idle

Automatic loading of loader and/or firmware files is deactivated.

Operating

Automatic loading of loader and/or firmware files is activated. When a USB medium is mounted, a suitable loader and/or firmware file us uploaded to the device. The USB medium is mounted when it is plugged into the USB port on the device, or when it is restarted.

If-unconfigured

Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

If-unconfigured

2.56.2 Config-and-script

This option activates the automatic loading of configuration and/or script files from a connected USB medium.

This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

A device can be fed with an undesirable configuration by resetting it to its factory settings and inserting a prepared USB data media. To prevent this you have to deactivated the reset switch.

Console path:

Setup > **Autoload**

Possible values:

Idle

Automatic loading of configuration and/or script files is deactivated.

Operating

Automatic loading of configuration and/or script files is activated. When a USB medium is mounted, a suitable configuration and/or script file us uploaded to the device. The USB medium is mounted when it is plugged into the USB port on the device, or when it is restarted.

If-unconfigured

Automatic loading of configuration and/or script files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

If-unconfigured

2.59 WLAN management

This menu is used to configure the WLAN management.

Console path:

Setup

2.59.1 Static-WLC-Configuration

Use this table to define the preferred wireless LAN controllers (WLCs) that this managed access point should contact. This setting is not required if the access point and WLC are located in the same IP network.

This setting is only relevant if at least one of the device's WLAN interfaces is switched to the 'Managed' operating mode.

Console path:

Setup > **WLAN-Management**

2.59.1.1 IP address

This is where the name of the CAPWAP service is defined that is used to trigger the WLAN controller via the DNS server.

The name is preset, so you do not need to change anything here. However, this parameter does offer the option of using the CAPWAP service of other manufacturers.

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.59.1.2 Port

This is where the name of the CAPWAP service is defined that is used to trigger the WLAN controller via the DNS server.

The name is preset, so you do not need to change anything here. However, this parameter does offer the option of using the CAPWAP service of other manufacturers.

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.59.1.3 Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If you have configured loopback addresses, you can specify them here as source address.

The sender address specified here is used **unmasked** for every remote station.

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

Name of the IP networks whose addresses are to be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If there is an interface called "DMZ", its address will be taken in this case).

LBO…LBF for the 16 loopback addresses.
Any IP address in the form `x.x.x.x`.

2.59.4 AutoWDS

This table contains the local factory settings of your device for the search for and the authentication at an AutoWDS base network. You use the timeout times to specify whether your device employs preconfigured integration, express integration, or a stepped combination of both.

As long as your device still has not received any AutoWDS settings from the WLC, the device uses the default settings specified here. However, as soon as the access point obtains an AutoWDS profile from a WLC, it takes a higher priority until the WLC revokes the configuration via CAPWAP or you reset the device.

The parameters specified here exclusively effect the initial login of an unassociated slave AP to a master AP for a subsequent search for a WLC. They do not affect the P2P links to a master AP that are set up later; your device uses the WLC configuration it obtains then.

You can check whether the device has received an AutoWDS configuration from the WLC with the status table **AutoWDS-Profile** (SNMP-ID 1.59.106).

Console path:

Setup > **WLAN-Management**

2.59.4.1 Operating

Switches the AutoWDS function on your device on/off. In the disabled state, the device does not attempt to autonomously integrate itself into a managed WLAN and also does not perform scans for an active AutoWDS network.

Console path:

Setup > **WLAN-Management** > **AutoWDS**

Possible values:

No
Yes

Default:

No

2.59.4.2 Preconf-SSID

Enter the SSID of the AutoWDS base network here. Your device will search here for a preconfigured integration. AutoWDS must be enabled and the *wait time until the preconfigured search* has to be set to higher than `0`.

After the wait time expires, the device switches all physical WLAN interfaces to client mode and starts the search for the SSID. If the device finds a matching SSID, it attempts to authenticate with the WPA2 passphrase entered for the corresponding WLAN.

The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to `0`.

Console path:

Setup > **WLAN-Management** > **AutoWDS**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.59.4.3 Preconf-Key

Specify the WPA2 passphrase that your device uses for authentication on the preconfigured AutoWDS base network.

The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to `0`.

Console path:

Setup > **WLAN-Management** > **AutoWDS**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default:

empty

2.59.4.4 Time-till-Preconf-Scan

Specify the wait time after which the AP switches to client mode and scans for an AutoWDS base network based on the corresponding values in the preconfiguration (the SSID and passphrase that are stored locally). This assumes that there are no configuration parts from a WLC available. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase and then perform the configuration procedure.

Parallel to this process, the configured *wait time for the start of express integration*.

The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to `0`.

Console path:

Setup > **WLAN-Management** > **AutoWDS**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables the wait time and the preconfigured integration procedure. The device immediately starts to count down the wait time for starting the express integration.

Default:

0

2.59.4.5 Time-till-Express-Scan

Specify the wait time after which the AP switches to client mode and scans for any AutoWDS base networks. This assumes that there no configuration parts from a WLC available and the *wait time for the start of the preconfigured integration* (if set) has expired. If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

Console path:

Setup > **WLAN-Management** > **AutoWDS**

Possible values:

0 … 4294967295 Seconds

Special values:

0

This value disables the wait time and the preconfigured integration procedure.

Default:

1

2.59.5 CAPWAP-Port

In this entry, you specify the CAPWAP port for the WLAN controller.

Console path:

Setup > **WLAN-Management**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:

1027

2.59.6 Log-Events

This parameter defines the categories that are written into the log of the device.

Console path:

Setup > **WLAN-Management**

Possible values:

Debug
Info
Warning
Error
StateChange
AutoWDS

2.59.120 Log-Entries

This parameter defines the maximum number of log entries for the device.

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 9999

Default:

200

2.60 Autoload

This menu is used to set up the automatic uploading of firmware, configurations or scripts from external data media or from a URL.

Console path:

Setup

2.60.1 Network

This menu is used to configure the automatic uploading of firmware, configurations or scripts over the network.

The settings defined here are used when the commands LoadFirmware, LoadConfig or LoadScript are entered at the command line. These commands upload firmware, configurations or scripts to the device with the help of the TFTP or HTTP(S) client.

Loading firmware, configurations or scripts with the help of the TFTP or HTTP(S) client can only succeed if the URL required to load the relevant file is fully configured and the URL is accessible when the command is executed. Alternatively, the URL can be entered as a parameter when the command is executed.

The values for Condition, URL and Minimum-Version set under /Setup/Autoload/Network constitute default values. These values are only used in cases where no other appropriate parameters are entered when the commands LoadFirmware, LoadConfig or Load Script are invoked on the command line.

Console path:

Setup > **Autoload**

2.60.1 Firmware

This menu is used to configure the automatic uploading of firmware over the network.

Console path:

Setup > **Autoload** > **Network**

2.60.1.1.1 Condition

This is where you select the condition under which the firmware specified under /Setup/Autoload/Network/Firmware/URL will be uploaded when the command LoadFirmware is executed.

If the command LoadFirmware is executed twice in succession with the setting "unconditionally", both memory locations will contain the same firmware version.

Console path:

Setup > **Autoload** > **Network** > **Firmware**

Possible values:

Unconditionally

The firmware will always be uploaded to and executed from the memory location of the inactive firmware. This setting deactivates version checking and the firmware specified will be uploaded in every case.

If different

The firmware is uploaded to and executed from the memory location for the inactive firmware if it is of a different version to the firmware active in the device and the inactive firmware. If the specified firmware is of the same version as one of the two existing firmware versions, then the firmware will not be

uploaded. The LoadFirmware command compares the firmware version (e.g. "8.10"), the release code (e.g. "RU1") and the file date.

If newer

The firmware is uploaded and executed only if it is newer than the firmware currently active in the device. The firmware is only uploaded to the memory location for the inactive firmware if it is newer than the active and inactive firmware versions on the device. If the specified firmware is older than one of the two existing firmware versions, then it will not be uploaded.

Default:

Unconditionally

2.60.1.1.2 Minimum version

Specify the minimum version of the firmware to be loaded over the network.

Firmware versions with a lower version number will be ignored.

Console path:

Setup > **Autoload** > **Network** > **Firmware**

Possible values:

Max. 14 characters from `[0-9].`

Default:

empty

2.60.1.1.3 URL

Specify the URL of the firmware (beginning with "tftp://", "http://" or "https://") that is to be uploaded over the network using the LoadFirmware command.

The TFTP or HTTP(S) client will only load the file specified here if the LoadFirmware command is entered without a URL as a parameter. Defining a URL as a parameter with the command allows a different file to be loaded specifically.

Console path:

Setup > **Autoload** > **Network** > **Firmware**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.60.1.1.4 Loopback-Address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

Console path:

Setup > **Autoload** > **Network** > **Firmware**

Possible values:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.60.1.2 Configuration

This menu contains the settings for uploading a configuration over the network.

Console path:

Setup > **Autoload** > **Network**

2.60.1.2.1 Condition

This is where you select the condition under **Setup** > **Autoload** > **Network** > **Configuration** > **URL** will be uploaded when the device is started.

Console path:

Setup > **Autoload** > **Network** > **Config**

Possible values:

Unconditionally

The configuration will always be uploaded.

If different

The configuration is uploaded only if it has a different version number than the configuration currently active in the device.

Default:

Unconditionally

2.60.1.2.2 URL

Specify the URL of the configuration file that is to be uploaded over the network.

Console path:

Setup > **Autoload** > **Network** > **Config**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.60.1.3 Script

This menu contains the settings for uploading a script over the network.

Console path:

Setup > **Autoload** > **Network**

2.60.1.3.1 Condition

This is where you select the condition under which the script specified under **Setup** > **Autoload** > **Network** > **Configuration** > **URL** will be uploaded when the command LoadScript is executed.

Console path:

Setup > **Autoload** > **Network** > **Script**

Possible values:

Unconditionally

The script will always be executed. This setting deactivates the checksum comparison and the specified script will always be uploaded unconditionally. In this case, the LoadScript command does not change the checksum for the most recently executed scripts as stored in the device.

If different

The script will only be executed if it differs from the last executed script. The difference to the last executed script is determined using a checksum. For this the complete script is always uploaded. The LoadScript command then compares the checksum of the uploaded script with the checksum of the last executed script stored in the device. When the script is executed, the LoadScript command updates the checksum stored in the device.

Default:

Unconditionally

2.60.1.3.2 URL

Specify the URL of the script file that is to be uploaded over the network.

Console path:

Setup > **Autoload** > **Network** > **Script**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.60.1.4 TFTP client

This menu contains the configuration for the TFTP client.

Console path:

Setup > **Autoload** > **Network**

2.60.1.4.1 Bytes-per-Hashmark

Here you can define after how many successfully uploaded bytes the TFTP client should display a hash mark (#) on the command line when executing LoadFirmware, LoadConfig or LoadScript. The TFTP client uses these hash marks to draw a progress bar when downloading firmware, configuration or script.

This value is only used when uploading via TFTP, not with HTTP or HTTPS. For HTTP or HTTPS, the hash character is sent max. every 100ms if progress has been made.

Console path:

Setup > **Autoload** > **Network** > **TFTP-Client**

Possible values:

Max. 4 characters from `[0-9]`

Default:

8192

2.60.1.5 SSL

This menu contains the encryption parameters for the network.

Console path:

Setup > **Autoload** > **Network**

2.60.1.5.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1

TLSv1.1

TLSv1.2

TLSv1.3

2.60.1.5.2 Key-exchange algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.60.1.5.3 Crypto-Algorithms

This entry specifies which cryptographic algorithms are allowed.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.60.1.5.4 Hash algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.60.1.5.5 Prefer PFS

This option means that your device always prefers to connect with PFS (Perfect Forward Secrecy), regardless of the default setting of the client.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

Yes
No

Default:

Yes

2.60.1.5.6 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

2.60.1.5.7 Elliptic curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1

secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.60.1.5.21 Signature hash algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **Autoload** > **Network** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.60.3 License

This menu is used to enter the information about the licensee, which the device enters into the registration form when LCOS carries out the automatic license activation.

Console path:

Setup > **Autoload**

2.60.3.1 URL

This setting specifies the URL of the license server used by the device for automatic license activation.

Console path:

Setup > **Autoload** > **License**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

http://www2.lancom.de/newoptionreg.nsf/RegOpt

2.60.3.2 Loopback-address

Optionally enter a different address here (name or IP) to send the reply message to the license server.

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Console path:

Setup > **Autoload** > **License**

Possible values:

Name of the IP network (ARF network), whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If an interface with the name "DMZ" already exists, the device will select that address instead.

LBO…LBF for one of the 16 loopback addresses or its name
Any IP address in the form `x.x.x.x`.

If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

2.60.3.10 Company

Enter the license owner's company here.

Console path:

Setup > **Autoload** > **License**

2.60.3.11 Surname

Enter the license owner's last name here.

Console path:

Setup > **Autoload** > **License**

2.60.3.12 First name

Enter the license owner's first name here.

Console path:

Setup > **Autoload** > **License**

2.60.3.13 Street and number

Enter the license owner's street and door number here.

Console path:

Setup > **Autoload** > **License**

2.60.3.14 Post code

Enter the license owner's post code here.

Console path:

Setup > **Autoload** > **License**

2.60.3.15 City

Enter the license owner's city here.

Console path:

Setup > **Autoload** > **License**

2.60.3.16 Country

Enter the license owner's country here.

Console path:

Setup > **Autoload** > **License**

2.60.3.17 E-Mail Address

Enter the licensee's e-mail address to which the license server sends its confirmation e-mail.

Console path:

Setup > **Autoload** > **License**

2.60.56 USB

This menu is used to configure the automatic uploading of firmware or configurations from an external USB data medium. Save the required configuration and/or script files in the "Config" directory located in the root directory of the connected USB medium.

Configuration and/or script files are only automatically loaded into the device if the device is in its factory default settings. A configuration reset can be used to return the device to its factory settings at any time.

Console path:

Setup > **Autoload**

2.60.56.1 Firmware-and-Loader

This option activates the automatic loading of loader and/or firmware files from a connected USB medium. Save the required loader and/or firmware files in the "Firmware" directory located in the root directory of the connected USB media.

This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

Console path:

Setup > **Autoload** > **USB**

Possible values:

Idle

Automatic loading of loader and/or firmware files is deactivated.

Operating

Automatic loading of loader and/or firmware files is activated. When a USB medium is mounted, a suitable loader and/or firmware file us uploaded to the device. The USB medium is mounted when it is plugged into the USB port on the device, or when it is restarted.

If-unconfigured

Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. A configuration reset can be used to return the device to its factory settings at any time.

Default:

If-unconfigured

2.63 Paket-Capture

This menu contains the settings for recording network data traffic via LCOScap and RPCAP.

Console path:

Setup

2.63.1 LCOSCap-Operating

This setting activates the LCOSCAP function.

Console path:

Setup > **Packet-Capture**

Possible values:

No
Yes

Default:

Yes

2.63.2 LCOSCap-Port

This setting specifies the port used by LCOSCAP.

Console path:

Setup > **Packet-Capture**

Possible values:

Max. 5 characters from `[0-9]`

Default:

41047

2.63.3 LCOSCap-Max.-Capture-Length

This setting determines the maximum length of the data packets recorded using LCOSCap.

Console path:

Setup > **Packet-Capture**

2.63.4 LCOSCap-Algorithms

This item is used to limit the range of encryption algorithms used for LCOSCap connections. The Simple algorithm uses the cleartext password as the basis for key derivation, while the other two algorithms use an encrypted password as the basis, which is encrypted with either SHA-256 or SHA-512. Simple must remain enabled for communicating with LCOS or LCOSCap versions before LCOS 10.40.

Note that the algorithm selection must be consistent with the selected password encryption algorithm: For example, if SHA-512 is used to encrypt admin passwords (see *2.11.89.2 Crypto-Algorithm* on page 384) and cleartext passwords are not stored (see *2.11.89.1 Keep-Cleartext* on page 384), SHA-512 must not be deactivated here, otherwise the device cannot be reached via LL2M.

Console path:

Setup > **Packet-Capture**

Possible values:

Simple
SHA-256
SHA-512

Default:

Simple

SHA-256

SHA-512

2.63.5 LCOSCap-WAN-Access

With this setting you control access to LCOSCAP from the WAN.

Console path:

Setup > **Packet-Capture**

Possible values:

No
No access allowed. This is the default for new devices or when the device is reset to factory settings.

Yes
Access granted. This is the default for devices that were updated from an older version to version LCOS 10.80.

VPN-Only
Access only allowed via VPN connections.

Default:

No

2.63.11 RPCap-Operating

This setting activates RPCAP. RPCAP is a protocol that is supported by (the Windows version of) Wireshark with which Wireshark can directly address the device. This makes the detour via a capture file unnecessary. In Wireshark you address the RPCAP interface using the sub-menu "Remote interfaces".

Console path:

Setup > **Packet-Capture**

Possible values:

No
Yes

Default:

No

2.63.12 RPCap-Port

This setting specifies the port used by RPCAP.

Console path:

Setup > **Packet-Capture**

Possible values:

0 … 65535

Default:

2002

2.63.13 RPCap-Blocking-TCP

This entry contains the setup values for RPCap-Blocking-TCP.

Console path:

Setup > **Packet-Capture**

2.63.14 RPCap-WAN-Access

With this setting you control access to RPCAP from the WAN.

Console path:

Setup > **Packet-Capture**

Possible values:

No

No access allowed. This is the default for new devices or when the device is reset to factory settings.

Yes

Access granted. This is the default for devices that were updated from an older version to version LCOS 10.80.

VPN-Only

Access only allowed via VPN connections.

Default:

No

2.63.20 Capture-to-File

This menu contains the settings for recording network data traffic to a USB drive in the PCAP format. This is used by Wireshark, for example.

Console path:

Setup > **Packet-Capture**

2.63.20.1 Files

In this table you configure the Wireshark traces on a connected USB drive.

Console path:

Setup > **Packet-Capture** > **Capture-to-File**

2.63.20.1.1 Name

Name of the entry.

Console path:

Setup > **Packet-Capture** > **Capture-to-File** > **Files**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.63.20.1.2 Operating

Defines whether the configuration entry is active or inactive.

Console path:

Setup > **Packet-Capture** > **Capture-to-File** > **Files**

Possible values:

No
Yes

2.63.20.1.3 File-Name

Full path and name of Wireshark capture file, e.g. `/usb/capture.pcap`.

Console path:

Setup > **Packet-Capture** > **Capture-to-File** > **Files**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.63.20.1.4 Interface

Name of the logical interface used for the Wireshark capture, e.g. DSL-1, LAN-1, etc.

Console path:

Setup > **Packet-Capture** > **Capture-to-File** > **Files**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.63.20.1.5 MAC-Address

MAC address to which the capture should be restricted, formatted without separators like "-" or ":".

Console path:

Setup > **Packet-Capture** > **Capture-to-File** > **Files**

Possible values:

Max. 17 characters from `[0-9a-e]`

2.64 PMS-Interface

You make all settings for the PMS interface (PMS = property management system) using the tables and parameters in this menu.

Console path:

Setup

2.64.1 Operating

Enable or disable the PMS interface for the device.

Console path:

Setup > **PMS-Interface**

Possible values:

No
Yes

Default:

No

2.64.2 PMS-Type

Identifies the protocol used by your property management system. Currently, the hotel property management systems from Micros Fidelio is supported via TCP/IP only.

Console path:

Setup > **PMS-Interface**

Possible values:

TCP/IP

Default:

TCP/IP

2.64.3 PMS server IP address

Enter the IPv4 address of your PMS server.

Console path:

Setup > **PMS-Interface**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

2.64.4 Loopback address

Optionally enter a different address here (name or IP) to send the reply message to the PMS server.

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Console path:

Setup > **PMS-Interface**

Possible values:

Name of the IP network (ARF network), whose address should be used.
"INT" for the address of the first intranet.
"DMZ" for the address of the first DMZ.

If an interface with the name "DMZ" already exists, the device will select that address instead.

LBO…LBF for one of the 16 loopback addresses or its name
Any IP address in the form `x.x.x.x`.

If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

2.64.5 PMS port

Enter the TCP port where your PMS server is accessible.

Console path:

Setup > **PMS-Interface**

Possible values:

0 … 65535

Default:

0

2.64.6 Separator

Using this entry you configure the separator that your PMS uses to transfer data records to an API. The Micros Fidelio specification, e.g., uses the pipe symbol by default (|, hex 7C).

You should not change this value if at all possible. An incorrect separator can lead to your PMS being unable to read the transmitted data records, and the PMS interface not working!

Console path:

Setup > **PMS-Interface**

Possible values:

Max. 1 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

|

2.64.7 Charset

Choose the character used by the PMS to transmit your guests' surnames to the device.

Console path:

Setup > **PMS-Interface**

Possible values:

CP850
W1252

Default:

CP850

2.64.8 Currency

If you offer fee-based Internet access, select the currency that you use to bill the time quotas that you offer (time quotas are set up using the tariff table). This unit is also displayed on the portal page. Please note that this currency must match the one on the PMS server.

Console path:

Setup > **PMS-Interface**

Possible values:

CENT
PENNY

Default:

CENT

2.64.10 Accounting

In this menu you configure the transfer of accounting information from your device to your PMS.

Console path:

Setup > **PMS-Interface**

2.64.10.1 Save-to-Flashrom

Enable or disable whether your device stores accounting information in regular intervals on the internal flash-ROM. By default this occurs hourly, but you can change the interval using the setup menu. Enable this option in order to prevent a complete loss of accounting information in case of a power outage.

Please note that frequent writing operations to this memory will reduce the lifetime of your device.

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

No
Yes

Default:

No

2.64.10.2 Save-to-Flashrom-Period

Using this entry you configure the interval that the device uses to store collected accounting information to the internal flash ROM.

Please note that frequent writing operations to this memory will reduce the lifetime of your device.

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

15

Special values:

0

The value `0` deactivates the function.

2.64.10.3 Cleanup-Accounting-Table-Period

Using this entry you configure the interval that the device uses to clean up expired sessions from the internal accounting table in the status menu.

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

60

Special values:

0

The value 0 disables the automatic cleanup.

2.64.10.4 Update-Accounting-Table-Period

Using this entry you configure the interval that the device uses to update the internal accounting table in the status menu.

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

15

Special values:

0

If the value is 0, the update is disabled and the status table does not display any values.

2.64.11 Login form

In this menu you make specific settings for the PMS for the login/portal pages which are displayed to your guests in case of unauthorized access attempts on the hotspot.

Console path:

Setup > **PMS-Interface**

2.64.11.1 PublicSpot-Login-Form

Enable or disable whether the portal page displays the Public Spot's own login screen. If you disable this setting, Public Spot users that use a combination of username and password as credentials (e.g., predefined or users with vouchers) can no longer login to the device.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

No
Yes

Default:

No

2.64.11.2 PMS-Login-Form

Choose the login page to be displayed by the portal page for your PMS interface.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

Free-of-charge
Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.

charge
Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate at the hotspot on the portal page with their username and room number, and also to select a rate.

free-VIP
Select this setting, if you want to offer your otherwise fee-based Internet access free of charge to VIPs. Although your VIPs see the login screen for fee-based access, they will not be billed any fees.

Default:

Free-of-charge

2.64.11.3 Fidelio-Free-Additional-check

Select the additional ID that a hotel guest uses – in addition to their username and room number – to authenticate on the Public Spot if you offer free Internet access. If you select `No-Check`, the device does not check for an additional ID.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

None

2.64.11.4 Fidelio-Charge-Additional-check

Select the additional ID used by a hotel guest – in addition to their username and room number – to authenticate on the Public Spot if you offer fee-based Internet access. If you select `No-Check`, the device does not check for an additional ID.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

Reservation number

2.64.11.5 Fidelio-Free-VIP-Additional-check

Select the additional ID used by a VIP – in addition to their username and room number – to authenticate on the Public Spot if you offer your VIPs free Internet access. If you select `No-Check`, the device does not check for an additional ID.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

None

2.64.11.6 Free-VIP-Status

In this table, you locally manage the VIP categories from your PMS.

Console path:

Setup > **PMS-Interface** > **Login-Form**

2.64.11.6.1 Status

Enter the VIP category from your PMS for the members that you want to provide with free Internet access.

For example, if you set up three VIP statuses (VIP1, VIP2, VIP3) for your PMS server, but you only want to offer hotel guests in category VIP2 free Internet access, enter the corresponding ID here.

Console path:

Setup > **PMS-Interface** > **Login-Form** > **Free-VIP-Status**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.64.11.14 User-Must-Accept-GTC

With this setting you enable or disable the confirmation of the terms of use on the PMS-login page.

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

No

The user is not prompted to accept the terms of use.

Yes

The user is prompted to accept the terms of use.

Default:

No

2.64.12 Guest-name-case-sensitive

Enable or disable whether the device checks the last name for capitalization (case sensitively) against the name of the guest in the PMS database during login. If this setting is enabled, the guest's Public Spot access is rejected if the spelling and capitalization of his name does not match that transferred by the hotel.

Console path:

Setup > **PMS-Interface**

Possible values:

No
Yes

Default:

Yes

2.64.13 Multi-Login

Enable or disable this if you want to allow a hotel guest to use the same credentials to login to the hotspot with multiple devices.

Console path:

Setup > **PMS-Interface**

Possible values:

No
Yes

Default:

Yes

2.64.15 Rate

Use this menu to configure the rates for the PMS interface.

Console path:

Setup > **PMS-Interface**

2.64.15.1 Rate

Enter the rate for the time quota, for example, `1`. Combined with the unit, this value corresponds to 1 hour, for example.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

0 … 4294967295

Default:

1

2.64.15.2 Unit

Select the unit for the time quota from the list.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Minutes
Hours
Days

Default:

Hours

2.64.15.3 Rate value

Enter the amount charged for the time quota. Combined with the selected currency, the value is 50 Cent, for example.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

0 … 4294967295

Default:

0

2.64.15.4 Name

Use this entry to specify a name for this rate.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.64.15.5 Tx bandwidth

Use this entry to restrict the transmit (Tx) bandwidth.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" disables the restriction of the transmit bandwidth.

2.64.15.6 Rx bandwidth

Use this entry to restrict the receive (Rx) bandwidth.

Console path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" disables the restriction of the receive bandwidth.

2.70 IPv6

This menu contains the settings for IPv6.

Console path:

Setup

2.70.1 Tunnel

Use this setting to manage the tunneling protocols to provide access to the IPv6 Internet via an IPv4 Internet connection.

Console path:

Setup > **IPv6**

2.70.1.1 6in4

The table contains the settings for the 6in4 tunnel.

Console path:

Setup > **IPv6** > **Tunnel**

2.70.1.1.1 Peer

Contains the name of the 6in4 tunnel.

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.1.1.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

0 … 65534

Default:

0

2.70.1.1.3 Gateway address

Contains the IPv4 address of the remote 6in4 gateway.

The 6in4 tunnel is only set up if the gateway can be reached by ping at this address.

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.70.1.1.4 IPv4-Rtg-tag

Here you specify the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4-Anycast-Address
- 6in4-Gateway-Address
- 6rd-Border-Relay-Address

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

0 … 65534

Default:

0

2.70.1.1.5 Gateway-IPv6-Address

Contains the IPv6 address of the remote tunnel endpoint on the intermediate network, for example, "2001:db8::1".

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:`

Default:

empty

2.70.1.1.6 Local-IPv6-Address

Contains the local IPv6 address of the device on the intermediate network, for example "2001:db8::2/64".

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:`

Default:

empty

2.70.1.1.7 Routed-IPv6-Prefix

Contains the prefix that is routed from the remote gateway to the local device and that is to be used in LAN, e.g. "2001:db8:1:1::/64" or "2001:db8:1::/48".

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:`

Default:

empty

2.70.1.1.8 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

Console path:

Setup > **IPv6** > **Tunnel** > **6in4**

Possible values:

No
Yes

Default:

Yes

2.70.1.2 6rd-Border-Relay

A router can operate as a 6rd client or as a 6rd border relay. A 6rd client or 6rd CE router (customer edge router) connects to an Internet service provider via a WAN connection and propagates the 6rd prefix to clients on the LAN. A 6rd border relay operates in the provider's network and connects 6rd clients to the IPv6 network. Thus a 6rd border relay used when an IPv6 connection is to be provided to 6rd routers.

Console path:

Setup > **IPv6** > **Tunnel**

2.70.1.2.1 Peer

Contains the name of the 6rd border relay tunnel.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.1.2.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

0 … 65534

Default:

0

2.70.1.2.3 IPv4-Loopback-Address

Set the IPv4 loopback address, i.e. the address where the device operates as a 6rd border relay.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.70.1.2.4 6rd prefix

Defines the prefix used by this border relay for the 6rd domain, e.g. 2001:db8:/32. This prefix must also be configured on all associated 6rd clients.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

Max. 16 characters from `A-Z][a-z][0-9]:/`

Default:

empty

2.70.1.2.5 IPv4-Mask-Length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

0 … 32

Default:

0

Special values:

0

The device uses the full IPv4 address.

2.70.1.2.6 DHCPv4 propagate

If you enable this function, the 6rd border relay distributes the prefix via DHCPv4 if the DHCPv4 client requests it.

If you do not enable this feature, you must manually configure the required 6rd settings for the 6rd clients.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

No
Yes

Default:

No

2.70.1.2.7 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Possible values:

No
Yes

Default:

Yes

2.70.1.3 6rd

The table contains the settings for the 6rd tunnel.

Console path:

Setup > **IPv6** > **Tunnel**

2.70.1.3.1 Peer

Contains the name of the 6rd tunnel.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.1.3.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

0 … 65534

Default:

0

2.70.1.3.3 Border-Relay-Address

Contains the IPv4 address of the 6rd-border relay.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.70.1.3.4 IPv4-Rtg-tag

Here you specify the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4-Anycast-Address
- 6in4-Gateway-Address

› 6rd-Border-Relay-Address

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

0 … 65534

Default:

0

2.70.1.3.5 6rd prefix

Contains the prefix used by the provider for 6rd services, e.g. 2001:db8::/32.

If the 6rd prefix is assigned through DHCPv4, you have to enter "::/32" here.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

Max. 24 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.1.3.6 IPv4-Mask-Length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

0 … 32

Default:

0

2.70.1.3.7 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

Console path:

Setup > **IPv6** > **Tunnel** > **6rd**

Possible values:

No
Yes

Default:

Yes

2.70.1.4 6to4

The table contains the settings for the 6to4 tunnel.

Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

Console path:

Setup > **IPv6** > **Tunnel**

2.70.1.4.1 Peer

Contains the name of the 6to4 tunnel.

Console path:

Setup > **IPv6** > **Tunnel** > **6to4**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.1.4.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **Tunnel** > **6to4**

Possible values:

0 … 65535

Default:

0

2.70.1.4.3 Gateway address

Contains the IPv4 address of the 6to4 relay or 6to4 gateway. Default value is the anycast address "192.88.99.1". In general, you can leave this address unchanged as it will always give you access to the closest 6to4 relay on the Internet.

The 6to4 tunnel is only set up if the gateway can be reached by ping at this address.

Console path:

Setup > **IPv6** > **Tunnel** > **6to4**

Possible values:

Max. 64 characters from `[0-9].`

Default:

192.88.99.1

2.70.1.4.4 IPv4-Rtg-tag

Here you specify the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4-Anycast-Address
- 6in4-Gateway-Address
- 6rd-Border-Relay-Address

Console path:

Setup > **IPv6** > **Tunnel** > **6to4**

Possible values:

0 … 65534

Default:

0

2.70.1.4.5 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

Console path:

Setup > **IPv6** > **Tunnel** > **6to4**

Possible values:

No
Yes

Default:

Yes

2.70.2 Router-Advertisement

These settings are used to manage the router advertisements, which are used to announce the device's availability as a router to the network.

Console path:

Setup > **IPv6**

2.70.2.1 Prefix options

The table contains the settings for IPv6 prefixes for each interface.

Console path:

Setup > **IPv6** > **Router-Advertisement**

2.70.2.1.1 Interface name

Defines the name of the logical interface.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.2.1.2 Prefix

Enter the prefix that is transmitted with the router advertisements, e.g. "2001:db8::/64".

The length of the prefix must always be exactly 64 bits ("/64"), or else the clients will not be able to generate their own addresses by adding their "interface identifier" (64 bits long).

If you wish to automatically use the prefix issued by the provider, then configure "::/64" here and enter the name of the corresponding WAN interface in the field **PD-Source**.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.1.3 Subnet ID

Here you set the subnet ID that is to be combined with the prefix issued by the provider.

If the provider assigns the prefix "2001:db8:a::/48", for example, and you assign the subnet ID "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64".

The maximum subnet length with a 48-bit long, delegated prefix is 16 bits (65,536 subnets of "0000" to "FFFF"). With a delegated prefix of "/56", the maximum subnet length is 8 bits (256 subnets of "00" to "FF").

In general, the subnet ID "0" is used when the WAN IPv6 address is compiled automatically. For this reason you should start with "1" when assigning subnet IDs for LANs.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

Max. 19 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.2.1.4 Adv.-OnLink

Indicates whether the prefix is "on link".

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

No
Yes

Default:

Yes

2.70.2.1.5 Adv.-Autonomous

Indicates whether a host can use the prefix for a "Stateless Address Autoconfiguration". If this is the case, it can connect directly to the Internet.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

No
Yes

Default:

Yes

2.70.2.1.6 PD-Source

Use the name of the interface that receives a prefix issued by the provider. This prefix is combined with the string entered in the field **Prefix** to form a subnet that announces router advertisements (DHCPv6 prefix delegation).

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.1.7 Adv.-Pref.-Lifetime

Defines the time in seconds for which an IPv6 address is "Preferred". The client also uses this lifetime for its generated IPv6 address. If the lifetime of the prefix has expired, the client no longer uses the corresponding IPv6 address. Is the "preferred lifetime" of an address expires, it will be marked as "deprecated". This address is then used only by already active connections until those connections end. Expired addresses are no longer available for new connections.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

0 … 2147483647

Default:

604800

2.70.2.1.8 Adv.-Valid-Lifetime

Defines the time in seconds, after which the validity of an IPv6 address expires. Expired addresses are no longer available for new connections.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

0 … 2147483647

Default:

2592000

2.70.2.1.9 DecrementLifetimes

If this option is enabled, the preferred and valid lifetime of the prefix in the router advertisements are automatically counted down over time or extended. The preferred and valid lifetimes of the prefix in the router advertisements are synchronized with the times from the delegated prefix as retrieved from the WAN. If the prefix from the provider is not updated, then the preferred and valid lifetimes are counted down to 0, and thus expire. As soon as the device updates the lifetimes of the delegated prefix from the WAN, then the prefix in the router advertisements is extended again. If this option is disabled, are preferred and valid lifetime from the delegated prefix are applied statically, but they not reduced or extended. This parameter has no effect on tunneled WAN connections (6to4, 6in4 and 6rd), because in this case the prefixes are not retrieved by DHCPv6 prefix delegation, and thus they have no lifetimes. Here, the statically-configured preferred and valid lifetimes from the prefix are applied. This parameter also has no effect if the value for PD source is left empty, because in this case there is no synchronization with the delegated WAN prefix.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Options**

Possible values:

No
Yes

Default:

Yes

2.70.2.2 Interface options

The table contains the settings for the IPv6 interfaces.

Console path:

Setup > **IPv6** > **Router-Advertisement**

2.70.2.2.1 Interface name

Defines the name of the logical interface to be used for sending router advertisements.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.2.2 Send adverts

Enables the periodic transmission of router advertisements and the response to router solicitations.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

No
Yes

Default:

Yes

2.70.2.2.3 Min-RTR-Interval

Defines in seconds the minimum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

3 … (0.75 * Max-RTR-Interval) seconds

Default:

200

2.70.2.2.4 Max-RTR-Interval

Defines in seconds the maximum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

4 … 1800 seconds

Default:

600

2.70.2.2.5 Managed-Flag

Sets the "Managed address configuration" flag in the router advertisement.

Setting this flag causes the clients to configure all addresses via "Stateful Autoconfiguration" (DHCPv6). In this case the clients also automatically retrieve other information, such as DNS server addresses.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

No
Yes

Default:

No

2.70.2.2.6 Other-Config-Flag

Sets the "Other configuration" flag in the router advertisement.

If this flag is set, the device instructs the clients to retrieve additional information (but not the addresses for the client) such as DNS server addresses via DHCPv6.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

No
Yes

Default:

Yes

2.70.2.2.7 Link-MTU

Here you set the valid MTU for the corresponding link.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

0 … 99999

Default:

1500

2.70.2.2.8 Reachable time

Specifies the time in milliseconds for which the router is considered to be reachable.

The default value of "0" means that the router advertisements have no specifications for reachable time.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

0 … 2147483647 Milliseconds

Default:

0

2.70.2.2.10 Hop limit

Defines the maximum number of routers to be used to forward a data packet. One router corresponds to one "hop".

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

0 … 255 Seconds

Default:

0

Special values:

0

No hop limit defined.

2.70.2.2.11 Def.-Lifetime

Specifies the time in seconds for which the router is considered to be reachable in the network.

If this value is set to **0**, the operating system will not use this router as the default router.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

0 … 2147483647 Seconds

Default:

1800

2.70.2.2.12 Default-Router-Mode

Defines how the device advertises itself as the default gateway or router.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

Auto

As long as a WAN connection exists, the router sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway. If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway. This behavior is compliant with RFC 6204.

Always

The router lifetime is always positive—i.e. greater than "0"—irrespective of the WAN connection status.

Never

The router lifetime is always "0".

Default:

Auto

2.70.2.2.13 Router-Preference

Defines the preference of this router. Clients enter this preference into their local routing tables.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

Low
Medium
High

Default:

Medium

2.70.2.2.14 RTR time

Specifies the time in milliseconds between successive transmissions of neighbor-solicitation messages to a neighbor if the address is being resolved or the accessibility is being tested.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Options**

Possible values:

0 … 4294967295 Milliseconds

Default:

0

2.70.2.3 Route options

The table contains the settings for the route options.

Console path:

Setup > **IPv6** > **Router-Advertisement**

2.70.2.3.1 Interface name

The table contains the settings for the route options.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Route-Options**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.3.2 Prefix

Set the prefix for this route. This should not exceed 64 bits in length if it is to be used for auto-configuration.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Route-Options**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.2.3.3 Route lifetime

Set how long in seconds the route should remain valid.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Route-Options**

Possible values:

0 … 65335 Seconds

Default:

0

Special values:

0

No route lifetime specified.

2.70.2.3.4 Route-Preference

This parameter specifies the priority of an advertised route. A router receiving a router advertisement with two routes of different preference will choose the route with the higher priority.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Route-Options**

Possible values:

Low
Medium
High

Default:

Medium

2.70.2.5 RDNSS options

This table contains the settings of RDNSS extension (recursive DNS server).

This function is not currently supported by Windows. Propagation of a DNS server, where required, is performed via DHCPv6.

Console path:

Setup > **IPv6** > **Router-Advertisement**

Possible values:

Low
Medium
High

Default:

Medium

2.70.2.5.1 Interface name

Name of the interface used by the device to announce information about the IPv6 DNS server in router advertisements.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **RDNSS-Options**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.5.2 Primary-DNS

Valid IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC 6106) for this interface.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **RDNSS-Options**

2.70.2.5.3 Secondary-DNS

Valid IPv6 address of the secondary IPv6 DNS server for this interface.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **RDNSS-Options**

2.70.2.5.4 DNS search list

This parameter defines which DNS search list the device propagates on this logical network.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **RDNSS-Options**

Possible values:

Internal

If you select this option, the device propagates either the DNS search list from the internal DNS server or the domain of this logical network. The domain is configured under **Setup** > **DNS** > **Domain**.

WAN

If you select this option, the device propagates the DNS search list from the provider (e.g. provider-xy.com) for this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under **Receive prefix from**.

Default:

Internal

2.70.2.5.5 Lifetime

Defines the time in seconds for which a client may use this DNS server for name resolution.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **RDNSS-Options**

Possible values:

0 … 65535

Default:

900

Special values:

0

Discontinuation

2.70.2.6 Prefix pools

In this directory you can define pools of prefixes for remote users and/or the corresponding RAS interfaces (PPTP, PPPoE). Define the prefixes for Ethernet interfaces under **Setup** > **IPv6** > **Router** > **Router-Advertisements** > **Prefix-Options** or in LANconfig under **IPv6** > **Router advertisement** > **Prefix list**.

Console path:

Setup > **IPv6** > **Router-Advertisement**

2.70.2.6.1 Interface name

Specify the name of the RAS interface applicable for this prefix pool.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.6.2 Start prefix pool

Here you specify the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., "2001:db8::". Each user is assigned precisely one /64 prefix from the pool.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

2.70.2.6.3 End prefix pool

Here you specify the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. '2001:db9:FFFF::'. Each user is assigned precisely one /64 prefix from the pool.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

::

2.70.2.6.4 Prefix-Length

Here you specify the length of the prefix assigned to the remote user by the router advertisement. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 3 characters from `0123456789`

Default:

64

2.70.2.6.5 Adv.-OnLink

Indicates whether the prefix is "on link".

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Yes
No

Default:

Yes

2.70.2.6.6 Adv.-Autonomous

Specifies whether the client can use the prefix for a stateless address auto-configuration (SLAAC).

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Yes
No

Default:

Yes

2.70.2.6.7 Adv.-Pref.-Lifetime

Specifies the time in seconds for which an IPv6 address is "Preferred". The client also uses this lifetime for its generated IPv6 address. If the lifetime of the prefix has expired, the client no longer uses the corresponding IPv6 address. Is the "preferred lifetime" of an address expires, it will be marked as "deprecated". This address is then used only by already active connections until those connections end. Expired addresses are no longer available for new connections.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 10 characters from `0123456789`

Default:

604800

2.70.2.6.8 Adv.-Valid-Lifetime

Defines the time in seconds, after which the validity of an IPv6 address expires. Expired addresses are no longer available for new connections.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

Possible values:

Max. 10 characters from `0123456789`

Default:

2592000

2.70.2.8 PREF64-Option

This table configures the prefix option (PREF64 option as per *RFC 8781*) for NAT64 prefixes, which are announced to clients in the router advertisement. Clients adopt this prefix e.g. for 464XLAT.

Console path:

Setup > **IPv6** > **Router-Advertisements**

2.70.2.8.1 Interface-Name

Specify the name of the interface to be used to advertise the PREF64 option.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.2.8.2 IPv6-Address-Prefixlength

Defines the NAT64 prefix with prefix length, e.g. 64:ff9b::/96

Console path:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

2.70.2.8.3 Scaled-Lifetime

Validity period of the NAT64 prefix in seconds.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1800

2.70.2.8.4 Comment

Enter a descriptive comment here.

Console path:

Setup > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3 DHCPv6

This menu contains the DHCPv6 settings.

Console path:

Setup > **IPv6**

2.70.3.1 Server

This menu contains the DHCP server settings for IPv6.

Console path:

Setup > **IPv6** > **DHCPv6**

2.70.3.1.2 Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.2.1 Address-Pool-Name

Specify the name of the address pool here.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.2.2 Start address pool

Here you specify the first address in the pool, e.g. "2001:db8::1"

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.2.3 End address pool

Here you specify the last address in the pool, e.g. "2001:db8::9"

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.2.5 Pref.-Lifetime

Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3600

2.70.3.1.2.6 Valid lifetime

Here you specify the time in seconds that the client should treat this address as "valid".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 10 characters from `[0-9]`

Default:

86400

2.70.3.1.2.7 PD-Source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.1.3 PD-Pools

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.3.1 PD-Pool-Name

Specify the name of the PD pool here.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.3.2 Start-PD-Pool

Here you specify the first prefix for delegation in the PD pool, e.g. "2001:db8:1100::"

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.3.1.3.3 End-PD-Pool

Here you specify the last prefix for delegation in the PD pool, e.g. "2001:db8:FF00::"

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.3.1.3.4 Prefix-Length

Here you set the length of the prefixes in the PD pool, e.g. "56" or "60"

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 3 characters from `[0-9]`

Default:

56

2.70.3.1.3.5 Pref.-Lifetime

Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3600

2.70.3.1.3.6 Valid lifetime

Here you specify the time in seconds that the client should treat this prefix as "valid".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 10 characters from `[0-9]`

Default:

86400

2.70.3.1.3.7 PD-Source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.1.4 Interface list

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.4.1 Interface-Name-or-Relay

From the list of LAN interfaces defined in the device, select the name of the interface on which the DHCPv6 server is working, for example "INTRANET".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.1.4.2 Operating

Activates or deactivates the DHCPv6 server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.1.4.3 Primary-DNS

IPv6 address of the primary DNS server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

::

2.70.3.1.4.4 Secondary-DNS

IPv6 address of the secondary DNS server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.3.1.4.5 Address-Pool-Name

Here you specify the address pool that the devices uses for this interface.

If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the table **Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.4.6 PD-Pool-Name

Specify the prefix-delegation pool that the devices is to use for this interface.

If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.1.4.7 Rapid commit

With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

The client must explicitly include the rapid commit option in its solicit message.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

No
Yes

Default:

No

Yes

2.70.3.1.4.8 Preference

Where multiple DHCPv6 servers are operated on the network, the preference parameter gives you the control over which server the clients will use. The primary server requires a higher preference value than the backup server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

0 … 255

Default:

0

2.70.3.1.4.9 Renew time

This specifies the time in seconds when the client should contact the server again (using a renew message) to extend the address/prefix received from the server. The parameter is also called T1.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

0 … 255

Default:

0

Special values:

0

Automatic

2.70.3.1.4.10 Rebind time

This specifies the time when the client should contact any server (using a rebind message) to extend its delegated address/prefix. The rebind event occurs only if the client receives no answer its renew request. The parameter is also called T2.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

0 … 255

Default:

0

Special values:

0

Automatic

2.70.3.1.4.11 Unicast address

Unicast address of the DHCP server. The DHCP server uses this address in the server unicast option to allow the client to communicate with to the server via unicast messages. By default, multicast is used.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

2.70.3.1.4.12 DNS search list

This parameter defines which DNS search list is sent to the clients by the DNS server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

None

The DNS server distributes no search lists to the clients.

Internal

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The system's own domain is configured under **Setup** > **IPv6** > **DNS** > **General-Settings**.

WAN

Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under Receive prefix from.

Default:

Internal

2.70.3.1.4.13 Reconfigure

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

However, if the WAN prefix changes, for example, due to disconnection and reconnection of an Internet connection or a request for a new prefix, the server has no way to inform the network devices that the prefix or address has changed. This means that a client is still using an old address or an old prefix, and can no longer communicate with the Internet.

The reconfigure feature allows the DHCPv6 server to require the clients in the network to request a renewal of leases / bindings.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

Possible values:

Off

Disables the reconfigure function

Reject

Clients that have used the Reconfigure Option in queries are rejected by the server and are not assigned an address, prefix or other options.

Allow

If the client sets the Reconfigure Option in queries, the server negotiates the necessary parameters with the client in order to start a reconfiguration at a later time.

Require

Clients have to set the Reconfigure Option in queries, otherwise the client rejects these clients. This mode is makes sense when you want to ensure that the server only serves clients which support Reconfigure. This ensure that all clients can use Reconfigure to update their addresses, prefixes, or other information at a later point in time.

Default:

Off

2.70.3.1.5 Limit-Confirm-To-Clients-With-Addresses

Using this setting you configure the behavior of the DHCPv6 server when it receives a confirm message from a client that does not yet have an IP address assigned to it. With the setting **no**, the server answers the message with a "Not-on-link" status; with the setting **yes**, it doesn't even answer.

This parameter is only required for development tests and is not relevant for normal operations.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

Possible values:

No
Yes

Default:

No

2.70.3.1.6 Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can define a reservation for each client in this table.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.6.1 Interface-Name-or-Relay

Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.1.6.2 Address or PD prefix

IPv6 address or PD prefix that you want to assign statically.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.1.6.3 Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- Specification as a client DUID, e.g. 0003000100a057000001
- Specification as a MAC address, e.g. 00a057000001
- Specification as an interface ID or remote ID, e.g. INTRANET

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

A hex string with max. 127 characters `[a-z][0-9]:-`

Default:

empty

2.70.3.1.6.5 Pref.-Lifetime

Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 10 characters from `[0-9]`

Default:

3600

2.70.3.1.6.6 Valid lifetime

Here you specify the time in seconds that the client should treat this prefix as "valid".

If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for preferred lifetime and valid lifetime. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 10 characters from `[0-9]`

Default:

86400

2.70.3.1.6.7 PD-Source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.3.1.6.8 Identifier-Type

This type specifies how the identifier in 2.70.3.1.6.3 is to be interpreted.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Client-ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

Mac-Address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface-ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote-ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

2.70.3.1.6.9 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.3.1.7 Create address routes

The DHCPv6 server creates an entry in the routing table for addresses assigned by IA_NA (identity association for non-temporary addresses). This function is required, for example, if the DHCPv6 server needs to assign IA_NA addresses to PPP interfaces and an IPv6 address pool is being used via multiple PPP interfaces. This switch is only required on point-to-point interfaces.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

Possible values:

No
Yes

Default:

No

2.70.3.1.8 Additional options

This is the **Additional options** table for the DHCP server.

In order for this option to be delivered to clients, the request sent by a client must must contain the corresponding option code.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.8.1 Interface-Name-or-Relay

Here you choose the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

Characters from the following character set:
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.70.3.1.8.2 Option code

Enter the code of your DHCPv6 option here.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

0 … 65535

Default:

0

2.70.3.1.8.3 Option type

Select the type of your DHCPv6 option here.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

String

The characters are accepted as a string. Please note: All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.

Integer8

An 8-bit integer from -128 to 127 optionally decimal, octal with prefix '0', or hexadecimal with prefix '0x'.

Integer16

A 16-bit integer from -32768 to 32767.

Integer32

A 32-bit integer from -2147483648 to 2147483647.

IPv6 address

IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses, such as ::ffff:1.2.3.4.

Domain list

All strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain always ends with the empty label 0.

Hexdump

Expects each block to have hex numbers only, without a leading 0x. Each block is filled with a leading 0 for an even length. The block is taken as **bigendian**.

2.70.3.1.8.4 Option value

Enter the contents of your DHCPv6 option here. The content must be formatted according to the selected option type.

Console path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

Depending on the option type, characters from:

```
[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

2.70.3.2 Client

This menu contains the DHCP client settings for IPv6.

Console path:

Setup > **IPv6** > **DHCPv6**

2.70.3.2.1 Interface list

This table determines the behavior of the DHCPv6 client.

Normally client behavior is controlled by the auto-configuration.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client**

2.70.3.2.1.1 Interface name

From the list of LAN interfaces defined in the device, specify the name of the interface that the DHCPv6 client operates on. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.2.1.2 Operating

Here you specify if and how the device enables the client.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

Autoconf

The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.

Yes

The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements.

No

The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

Default:

Autoconf

2.70.3.2.1.3 Request DNS

Here you specify whether the client should query the DHCPv6 server for DNS servers.

You must enable this option in order for the device to obtain information about a DNS server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.2.1.4 Request address

Here you specify whether the client should query the DHCPv6 server for an IPv6 address.

Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i.e. not distributed by 'SLAAC'.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.2.1.5 Request PD

Here you specify whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

No

2.70.3.2.1.6 Rapid commit

When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.2.1.7 Send FQDN

With this setting you specify whether the client should send its device name using the FQDN option (Fully Qualified Domain Name) or not.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.2.1.8 Accept-Reconf

With this setting you specify whether the client of the corresponding interface can negotiate a Reconfigure with the DHCPv6 server.

If you enable this setting, you allow a DHCP server to send a reconfigure message to a client. On its part, the client answers the server with renew or rebind. In the response to this renew or rebind, the server can then assign the client a new IPV6 address or IPv6 prefix, or prolong it.

You can find further information about dynamic reconfiguration in the Reference Manual under "Reconfigure" in the IPv6 section for the DHCPv6 server.

In order for dynamic reconfiguration to work, you also have to enable it on the server!

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

No

2.70.3.2.1.9 Request domain list

With this setting you specify whether a client should call up the list of the available domain names from the DHCP server using the appropriate interface.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

No
Yes

Default:

Yes

2.70.3.2.1.10 Request SNTP

Specify whether the DHCPv6 client requests a list of SNTP (Simple Network Time Protocol) servers from the DHCPv6 server.

This requires regular synchronization with a timeserver.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

0

No

1

Yes

Default:

0

2.70.3.2.1.11 PD hint

Here you specify whether the DHCPv6 client requests a desired prefix length from the DHCPv6 server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

Three characters from the following character set: `[0-9]`

2.70.3.2.2 User class identifier

This assigns the device a unique user class ID.

A user class identifier is used to identify the type or category of client to the server. For example, the user class identifier can be used to identify all clients of people in the accounting department, or all printers at a specific location.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.2.3 Vendor class identifier

This assigns the device a unique vendor class ID.

The vendor-class-identifier is used to identify the manufacturer of the hardware running the DHCP client.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

Manufacturer name

2.70.3.2.4 Vendor-Class-Number

Determines the enterprise number that the device manufacturer used to register with the Internet Assigned Numbers Authority (IANA).

Console path:

Setup > **IPv6** > **DHCPv6** > **Client**

Possible values:

Max. 10 characters from `[0-9]`

Default:

2356

2.70.3.2.5 Additional-Options

In this table certain options can be configured for the DHCPv6 client.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client**

2.70.3.2.5.1 Interface-Name

Interface that the DHCPv6 client should use for this option, e.g. WAN remote site or IPv6 LAN network.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Additional-Options**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.2.5.2 Option-Number

Specifies the assigned IANA number of the DHCP option as defined in the RFC.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Additional-Options**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.70.3.2.5.3 Option-Type

Specifies the type of the DHCPv6 option.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Additional-Options**

Possible values:

Integer8
Integer16
Integer32
IPv6 addresses
Domain-List
String
Hexdump
Do-not-send

This option type means that no option content is sent, only the option number in the option request if no option value is provided in the RFC.

2.70.3.2.5.4 Option-Value

Specifies the content of the DHCPv6 option.

A comma and/or space-separated list can also be specified, except in the case of a string. For integer values the C-codes for numbers apply, i.e. 0x results in a hex value and if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: Elapsed-Time, Server-DUID, Reconfigure-Accept and Rapid-Commit.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Additional-Options**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.2.5.5 Request-Option

Specifies whether the DHCPv6-Option-Request should request the option number. The behavior is defined via the respective RFC of the DHCPv6 option.

Console path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Additional-Options**

Possible values:

Yes
No

2.70.3.3 Relay agent

This menu contains the DHCP relay agent settings for IPv6.

Console path:

Setup > **IPv6** > **DHCPv6**

2.70.3.3.1 Interface list

This table determines the behavior of the DHCPv6 relay agent.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent**

2.70.3.3.1.1 Interface name

From the list of LAN interfaces defined in the device, specify the name of the interface where the relay agent receives requests from DHCPv6 clients, for example "INTRANET".

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.3.3.1.2 Operating

With this option you define if and how the device enables the relay agent.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

No
Relay agent is not enabled.

Yes
Relay agent is enabled.

Default:

Yes

2.70.3.3.1.3 Interface address

Specify the relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.1.4 Dest-Address

Define the IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

You can define additional server targets via *2.70.3.3.1.6 Dest-Address-2* on page 1579, *2.70.3.3.1.8 Dest-Address-3* on page 1580 and *2.70.3.3.1.10 Dest-Address-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

ff02::1:2

2.70.3.3.1.5 Dest-Interface

Here you specify the destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

You can define additional server targets via *2.70.3.3.1.7 Dest-Interface-2* on page 1579, *2.70.3.3.1.9 Dest-Interface-3* on page 1580 and *2.70.3.3.1.11 Dest-Interface-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.1.6 Dest-Address-2

Define a second IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

You can define additional server targets via *2.70.3.3.1.4 Dest-Address* on page 1578, *2.70.3.3.1.8 Dest-Address-3* on page 1580 and *2.70.3.3.1.10 Dest-Address-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

empty

2.70.3.3.1.7 Dest-Interface-2

Here you specify a second destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

You can define additional server targets via *2.70.3.3.1.5 Dest-Interface* on page 1578, *2.70.3.3.1.9 Dest-Interface-3* on page 1580 and *2.70.3.3.1.11 Dest-Interface-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.1.8 Dest-Address-3

Define a third IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

You can define additional server targets via *2.70.3.3.1.4 Dest-Address* on page 1578, *2.70.3.3.1.6 Dest-Address-2* on page 1579 and *2.70.3.3.1.10 Dest-Address-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

empty

2.70.3.3.1.9 Dest-Interface-3

Here you specify a third destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

You can define additional server targets via *2.70.3.3.1.5 Dest-Interface* on page 1578, *2.70.3.3.1.7 Dest-Interface-2* on page 1579 and *2.70.3.3.1.11 Dest-Interface-4* on page 1581.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.1.10 Dest-Address-4

Define a fourth IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

You can define additional server targets via *2.70.3.3.1.4 Dest-Address* on page 1578, *2.70.3.3.1.6 Dest-Address-2* on page 1579 and *2.70.3.3.1.8 Dest-Address-3* on page 1580.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]:`

Default:

empty

2.70.3.3.1.11 Dest-Interface-4

Here you specify a fourth destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

You can define additional server targets via *2.70.3.3.1.5 Dest-Interface* on page 1578, *2.70.3.3.1.7 Dest-Interface-2* on page 1579 and *2.70.3.3.1.9 Dest-Interface-3* on page 1580.

In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.1.12 Dest-Loopback

Specify here an optional sender address that the relay agent uses for packets towards the DHCPv6 server.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.3.3.2 Create address routes

The DHCPv6 server creates an entry in the routing table for addresses assigned by IA_NA (identity association for non-temporary addresses). This function is required, for example, if the DHCPv6 server needs to assign IA_NA addresses to PPP interfaces and an IPv6 address pool is being used via multiple PPP interfaces. This switch is only required on point-to-point interfaces.

Console path:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent**

Possible values:

No
Yes

Default:

No

2.70.4 Network

Here you can adjust further IPv6 network settings for each logical interface supported by your device.

Console path:

Setup > **IPv6**

2.70.4.1 Addresses

This table is used to manage the IPv6 addresses.

Console path:

Setup > **IPv6** > **Network**

2.70.4.1.1 Interface name

Give a name to the interface that you want to assign the IPv6 network.

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.4.1.2 IPv6-Address-Prefixlength

Specify an IPv6 address including the prefix length for this interface.

The default prefix length is 64 bits ("/64"). If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device are designed for a maximum length of 64 bits.

A possible address is, for example, "2001:db8::1/64". An interface can have multiple IPv6 addresses:

- A "global unicast address", e.g. "2001:db8::1/64",
- A "unique local address", e.g. "fd00::1/64".

"Link local addresses" are fixed and not configurable.

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.4.1.3 Address type

Specify the type of IPv6 address.

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Unicast

With the Unicast address type, you use the field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583 to specify a full IPv6 address along with its interface identifier, e.g. “2001:db8::1234/64”.

Anycast

With the Anycast address type, you can also use the field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583 to specify a full IPv6 address along with its interface identifier, e.g. “2001:db8::1234/64”. Internally, the device handles this address as an anycast address.

EUI-64

The IPv6 address is formed according to the IEEE standard “EUI-64”. The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: “2001:db8:1::/64”.

EUI-64 ignores any value set as “interface identifier” in the corresponding IPv6 address and replaces it with an “interface identifier” as per EUI-64.

The prefix length for EUI-64 must be "/64".

Delegated-Auto-Configuration

The IPv6 address is formed from the router advertisement prefix received on the selected interface (field *2.70.4.1.1 Interface name* on page 1582) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583. The field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583 can be filled out e.g. with the value" ::2/64" in combination with the prefix "2001:db8::/64" on the interface to form the address "2001:db8::2/64".

Delegated-DHCPv6

The IPv6 address is formed from the delegated DHCPv6 prefix received on the selected interface (field *2.70.4.1.1 Interface name* on page 1582) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583. The field *2.70.4.1.2 IPv6-Address-Prefixlength* on page 1583 can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/56" on the interface to form the address "2001:db8::2/64". Similarly, an address can be formed from any subnet of the delegated prefix, e.g "0:0:0:0001::1" and the prefix "2001:db8::/56" go to form the address "2001:db8:0:0001::1/64".

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

Unicast

2.70.4.1.4 Network group

Enter a descriptive name for this combination of IPv6 address and prefix. This label of the network group does not have to be unique. Consequently, several different prefixes can belong to a network group.

For example, the network group can be referenced in the IPv6 firewall in the station table **Setup** > **IPv6** > **Firewall** > **Stations** in the column **Local network** if the **Type** there is set to "Local network". The station then consists of all prefixes in this network group.

You can also reference it in the VPN in the table **Setup** > **VPN** > **Networks** > **IPv6-Rules** in the column **Local network**. As a result, all prefixes of the network group end up on the local side of the network relationship.

Entering a network group is optional.

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.4.1.5 Comment

Enter a descriptive comment for this entry.

Entering a comment is optional.

Console path:

Setup > **IPv6** > **Network** > **Addresses**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.4.2 Parameter

This table is used to manage the IPv6 parameters.

Console path:

Setup > **IPv6** > **Network**

2.70.4.2.1 Interface name

Give a name to the interface for which the IPv6 parameters are to be configured.

Console path:

Setup > **IPv6** > **Network** > **Parameter**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.4.2.2 IPv6 gateway

Specify the IPv6 gateway to be used by this interface. Use a global unicast address (e.g. 2001:db8::1) or a link-local address to which you add to the corresponding interface (%<INTERFACE>, e.g. fe80::1%INTERNET).

This parameter overrides gateway information that the device may receive via router advertisements, for example.

Console path:

Setup > **IPv6** > **Network** > **Parameter**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

::

2.70.4.2.3 Primary-DNS

Specify the primary IPv6 DNS server to be used by this interface.

Console path:

Setup > **IPv6** > **Network** > **Parameter**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

::

2.70.4.2.3 Secondary-DNS

Specify the secondary IPv6 DNS server to be used by this interface.

Console path:

Setup > **IPv6** > **Network** > **Parameter**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]/:`

Default:

::

2.70.4.3 Loopback

You can set IPv6 loopback addresses here. The device sees each of these addresses as its own address, which is also available if a physical interface is disabled, for example.

Console path:

Setup > **IPv6** > **Network**

2.70.4.3.1 Name

Enter a unique name for this loopback address.

Console path:

Setup > **IPv6** > **Network** > **Loopback**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.4.3.2 IPv6-Loopback-Addr.

Enter a valid IPv6 address here.

Console path:

Setup > **IPv6** > **Network** > **Loopback**

Possible values:

Max. 39 characters from `0123456789ABCDEFabcdef:./`

Default:

empty

2.70.4.3.3 Rtg-Tag

Here you specify the routing tag of the network that the loopback address belongs to. Only packets with this routing tag will reach this address.

Console path:

Setup > **IPv6** > **Network** > **Loopback**

Possible values:

Max. 5 characters from `0123456789`

Default:

0

2.70.4.3.4 Comment

You have the option to enter a comment here.

Console path:

Setup > **IPv6** > **Network** > **Loopback**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5 Firewall

This menu contains the settings for the firewall.

Console path:

Setup > **IPv6**

2.70.5.1 Operating

Enables or disables the firewall.

This item enables the firewall globally. The firewall is only active if you enable it here. If you disable the firewall here and at the same time enable it for individual interfaces, it remains disabled for all interfaces.

Console path:

Setup > **IPv6** > **Firewall**

Possible values:

No
Yes

Default:

Yes

2.70.5.2 Forwarding rules

This table contains the rules that the firewall will apply for forwarding data.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.2.1 Name

This table contains the rules that the firewall will apply for forwarding data.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.2.2 Flags

These options determine how the firewall handles the rule.

You can select several options at the same time.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Disabled

The rule is deactivated. The firewall skips this rule.

Linked

After processing the rule, the firewall looks for additional rules which come in question.

Stateless

This rule does not take the statuses of the TCP sessions into account.

LB-Switchover

Specifies whether the sessions under these rules should be moved to a better line as identified by Dynamic Path Selection. This is only possible for unmasked connections, e.g. VPN connections.

2.70.5.2.3 Prio

This information determines the priority with which the firewall applies the rule. A higher value determines a higher priority.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

2.70.5.2.4 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.70.5.2.5 Action

Specifies the action that the firewall performs if the rule condition is true. There are certain standard actions already specified in the table **Setup** > **IPv6** > **Firewall** > **Actions**. In addition, you can also define your own actions.

You can enter multiple actions, separated by commas.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

REJECT

2.70.5.2.7 Services

This information determines for which services the firewall applies this rule. There are certain services already specified in the table **Setup** > **IPv6** > **Firewall** > **Actions**. In addition, you can also define your own services.

You can enter multiple actions, separated by commas.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

ANY

2.70.5.2.8 Source stations

This information determines for which source stations the firewall applies this rule. There are certain stations already specified in the table **Setup** > **IPv6** > **Firewall** > **Stations**. In addition, you can also define your own stations.

You can enter multiple actions, separated by commas.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

ANYHOST

2.70.5.2.9 Destination stations

This information determines, for which destination stations the firewall applies this rule. There are certain stations already specified in the table **Setup** > **IPv6** > **Firewall** > **Stations**. In addition, you can also define your own stations.

You can enter multiple actions, separated by commas.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

ANYHOST

2.70.5.2.10 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.5.2.11 Src-Tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received. This can be used to restrict firewall rules to certain ARF contexts.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

0 … 65535

Default:

0

Special values:

65535

The firewall rule is applied if the expected interface- or routing tag is 0.

65534

The firewall rule is applied if the expected interface- or routing tag is 1...65534.

0

Wildcard. The firewall rule is applied to all ARF contexts (the expected interface- or routing tag is 0...65535).

2.70.5.2.12 LB-Policy

Defines the Dynamic Path Selection Policy used for this firewall rule. This can either be one of the predefined ones from *2.8.20.4 Predefined-Selectors* on page 259 or one of the self-generated ones under *2.110.4.16 Policies* on page 1883.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.3 Action list

In this table, you can group actions. Define the actions you previously under **Setup** > **IPv6** > **Firewall** > **Actions**.

You can not delete an action in this list if the firewall is used in a forwarding or inbound rule.

Console path:

Setup > **IPv6** > **Firewall** > **Forwarding-Rules**

2.70.5.3.1 Name

Specifies the name of a group of actions.

Console path:

Setup > **IPv6** > **Firewall** > **Action-List**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.3.2 Description

Contains the list of actions that are grouped together under this group name.

Separate the individual entries with a comma.

Console path:

Setup > **IPv6** > **Firewall** > **Action-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.5.5 Station list

You can group stations in this table. Define the actions previously under **Setup** > **IPv6** > **Firewall** > **Stations**.

You can not delete a station in this list if the firewall is used in a forwarding or inbound rule.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.5.1 Name

Specifies the name of a group of stations.

Console path:

Setup > **IPv6** > **Firewall** > **Stations-List**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.5.5.2 Description

Contains the list of stations that are grouped together under this group name.

Separate the individual entries with a comma.

Console path:

Setup > **IPv6** > **Firewall** > **Stations-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.5.6 Service list

You can group services in this table. Define the services previously under **Setup** > **IPv6** > **Firewall** > **Services**.

You can not delete a service in this list if the firewall is used in a forwarding or inbound rule.

Console path:

Setup > **IPv6** > **Firewall** > **Stations-List**

2.70.5.6.1 Name

Specifies the name of a group of services.

Console path:

Setup > **IPv6** > **Firewall** > **Service-List**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.6.2 Description

Contains the list of services that are grouped together under this group name.

Separate the individual entries with a comma.

Console path:

Setup > **IPv6** > **Firewall** > **Service-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.7 Actions

The firewall can perform the forwarding and inbound rule actions for the actions contained in this table.

You can combine multiple actions under **Setup** > **IPv6** > **Firewall** > **Actions-list**.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.7 Name

Specifies the name of the action.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.7.2 Limit

When this limit is exceeded, the firewall applies the filter rule.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The rule will come into force immediately.

2.70.5.7.3 Unit

When this limit is exceeded, the firewall applies the filter rule.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

kBit
kByte
Packets
Sessions
Bandwidth (%)

Default:

Packets

2.70.5.7.4 Time

Determines the measurement period that the firewall applies to the limit.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Second
Minute
Hour
Absolute

Default:

Absolute

2.70.5.7.5 Context

Determines the context that the firewall applies to the limit.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Session
The limit only applies to the data traffic for the current session.
Station
The limit only applies to the data traffic for this station.
Global
All sessions to which this rule applies use the same limit counter.

Default:

Session

2.70.5.7.6 Flags

Determines the properties of the limits of the action.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Reset
If the limit is exceeded, the action resets the counter.

Shared

All rules to which this limit applies use the same limit counter.

2.70.5.7.7 Action

Determines the action the firewall performs when the limit is reached.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Reject

The firewall rejects the data packet and sends an appropriate notification to the sender.

Drop

The firewall discards the data packet without notification.

Accept

The firewall accepts the data packet.

Default:

Reject

2.70.5.7.10 Content-Filter

Defines the content filter profile.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

CF-BASIC-PROFILE

Default:

CF-PARENTAL-CONTROL-PROFILE

Default:

CF-WORK-PROFILE

2.70.5.7.11 DiffServ

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.

Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

BE
EF
CS0 to CS7
AF11 to AF43
No
Value

You can enter the DSCP decimal value directly in the **DSCP value** field.

Default:

No

2.70.5.7.12 DSCP value

Determines the value for the Differentiated Services Code Point (DSCP).

If you selected the "Value" option in the **DiffServ** field, enter a value here.

Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 2 characters from `[0-9]`

Default:

empty

2.70.5.7.13 Conditions

Determines which conditions must be met in order for the action to be performed. Define the conditions under **Setup** > **IPv6** > **Firewall** > **Conditions**.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.7.14 Trigger actions

Determines which trigger actions the firewall should start in addition to filtering the data packets. Define the trigger actions under **Setup** > **IPv6** > **Firewall** > **Trigger-actions**.

Console path:

Setup > **IPv6** > **Firewall** > **Actions**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.9 Stations

The firewall can perform the forwarding and inbound rule actions for inbound connections from the source stations listed in this table.

You can combine multiple stations under **Setup** > **IPv6** > **Firewall** > **Station-list**.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.9.1 Name

Specifies the name of the station.

Console path:

Setup > **IPv6** > **Firewall** > **Stations**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.9.2 Type

Determines the station type. Your selection determines which of the following table columns (*>Local-network*, *Remote-peer/local-host* and *Address/Prefix*) must be filled out.

Console path:

Setup > **IPv6** > **Firewall** > **Stations**

Possible values:

Local-network

Name of a local network, e.g. INTRANET.

- Only the column *Local-network* has to be filled out.
- If it contains an interface name, then the station consists of all networks on this interface.
- If you specify a network group, then the station consists of all prefixes under *Addresses* with this group.

Remote-peer

Name of a WAN remote site, e.g. INTERNET.

- Only the column *Remote-peer/local-host* has to be filled out.
- It can contain a WAN interface or a RAS template. With a WAN interface it resolves to all prefixes/networks to which a route exists via this WAN interface, and with a RAS template it resolves to all prefixes/networks to which a route exists via a RAS interface from this template.

Prefix

IPv6 prefix

- Only the column *Address/Prefix* has to be filled out.
- It contains an IPv6 prefix, e.g. "2001:db8::/32".

Identifier

- The columns *Local-network* and *Address/Prefix* both have to be filled out
- *Local-network* contains a WAN interface or a RAS template.
- *Address/Prefix* contains an IPv6 identifier. These are the last 64 bits of the IPv6 address of an IPv6 host, e.g. "::2a0:57ff:fe1b:3a6a". The value must contain two leading colons.
- This identifier forms an address when combined with the networks of the interface under *Local-network* or with the RAS interface from the specified template.
- Furthermore, a link-local address with this identifier is formed for each of these interfaces.

IP-Address

- Only the column *Address/Prefix* has to be filled out.
- It contains an IPv6 address, e.g. "2001:db8::/1".

Named-host

Name of a local IPv6 host or local station.

- The column *Remote-peer/local-host* must be filled out and contains a hostname.
- The column *Local-network* is optional and can include a LAN interface.
- The host name is resolved to a host address using the DHCPv6 server or the DNS server in the device.
- If an interface has been specified, the address is only taken if it can be reached via this interface.

MAC-Address

This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

- The column *Local-network* is optional and can contain the name of a network where the station object is located.
- The column *Address/Prefix* contains the MAC address used to identify the object.

In rules, MAC addresses can be a source but not a target.

Delegated-prefix

Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

- The *Local-network* column is optional and can contain the name of a network where the station object is located. This can be used as a restriction on the local network.
- The column *Remote-peer/local-host* is required and should contain the remote peer from which the delegated prefix is obtained or derived.
- The column *Address/Prefix* contains a prefix or address that is linked (OR operator) with the prefix obtained from the provider. If the object should refer to the entire prefix, you can either configure ::/0 or the entry can be left blank.

  Example: The provider delegates the prefix 2001:db8:1234::/48 to the remote peer INTERNET.

  - To use the subnet abcd, the *Address/Prefix* has to be configured as the value 0:0:0:abcd::/48.
  - If the address to be used is 2001:db8:0:23::dead:beef/128, then the *Address/Prefix* can be configured as 0:0:0:23::dead:beef/128.
  - If the entire prefix is to be used, then the *Address/Prefix* can be configured as ::/0 or the entry can be left blank.

Default:

Local-network

2.70.5.9.3 Local network

If you selected the appropriate option in the **Type** field, you enter the name of the local network here.

Console path:

Setup > **IPv6** > **Firewall** > **Stations**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.9.6 Remote peer/local host

If you selected the appropriate option in the **Type** field, you enter the name of the remote peer or local host here.

Console path:

Setup > **IPv6** > **Firewall** > **Stations**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.9.7 Address/prefix

If you selected the appropriate option in the **Type** field, enter the IP address or prefix of the station here.

Console path:

Setup > **IPv6** > **Firewall** > **Stations**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

2.70.5.10 Services

The firewall can perform the forwarding and inbound rule actions for the connection protocols of the services listed in this table.

You can combine multiple services under **Setup** > **IPv6** > **Firewall** > **Service-list**.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.10.1 Name

Specifies the name of the service.

Console path:

Setup > **IPv6** > **Firewall** > **Services**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.10.2 Protocol

Specifies the protocol of the service.

Console path:

Setup > **IPv6** > **Firewall** > **Services**

Possible values:

TCP+UDP
TCP
UDP

Default:

TCP+UDP

2.70.5.10.3 Ports

Specifies the port for the service. Separate multiple ports with a comma.

Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

Console path:

Setup > **IPv6** > **Firewall** > **Services**

Possible values:

Max. 64 characters from `[0-9],`

Default:

empty

2.70.5.10.4 Src-Ports

Determines whether the specified ports are source ports.

In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

Console path:

Setup > **IPv6** > **Firewall** > **Services**

Possible values:

No
Yes

Default:

No

2.70.5.11 Protocols

The firewall can perform the forwarding and inbound rule actions for the protocols listed in this table.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.11.1 Name

Specifies the name of the protocol.

Console path:

Setup > **IPv6** > **Firewall** > **Protocols**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.11.2 Protocol

Specifies the protocol number.

Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

Console path:

Setup > **IPv6** > **Firewall** > **Protocols**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.70.5.12 Conditions

The firewall can perform the forwarding and inbound rule actions for the conditions listed in this table.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.12.1 Name

The firewall can perform the forwarding and inbound rule actions for the conditions listed in this table.

Console path:

Setup > **IPv6** > **Firewall** > **Conditions**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.12.2 Conditions

Specifies the conditions which must be met.

Console path:

Setup > **IPv6** > **Firewall** > **Conditions**

Possible values:

Not connected
Default route
Backup connection
VPN route
Transmitted
Received

2.70.5.12.3 Transport direction

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

Console path:

Setup > **IPv6** > **Firewall** > **Conditions**

Possible values:

Physical
Logical
Backup connection
VPN route
Transmitted
Received

Default:

Physical

2.70.5.12.4 DiffServ

Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Console path:

Setup > **IPv6** > **Firewall** > **Conditions**

Possible values:

Ignore
BE
EF
CS0 to CS7, CSx

CSx extends the range to all class selectors.

AF11 to AF43, AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx

AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx extends the range to the corresponding assured-forwarding classes (e.g.,AF1x takes the classes AF11, AF12, AF13 into account).

No
Value

You can enter the DSCP decimal value directly in the **DSCP value** field.

Default:

Ignore

2.70.5.12.5 DSCP value

Determines the value for the Differentiated Services Code Point (DSCP).

If you selected the "Value" option in the **DiffServ** field, enter a value here.

Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Console path:

Setup > **IPv6** > **Firewall** > **Conditions**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

2.70.5.13 Trigger actions

This table contains a list of the trigger actions, which the firewall actions can start.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.13.1 Name

Specifies the name of the trigger action.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.5.13.2 Notifications

Determines whether and how a notification should be sent.

If you want to receive e-mail notifications, you must enter an e-mail address in **Setup** > **IP-Router** > **Firewall** > **Admin-Email**.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

SNMP
SYSLOG
E-mail

2.70.5.13.3 Disconnect

Determines whether the firewall disconnects the connection to the remote station if the filter condition is true.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

No
Yes

Default:

No

2.70.5.13.4 Block source

Determines whether the firewall disconnects the source if the filter condition is true. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the **Host-lock-list** under **Status** > **IPv6** > **Firewall**.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

No
Yes

Default:

No

2.70.5.13.5 Block time

Specifies how many minutes the firewall blocks the source.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

Max. 8 characters from `[0-9]`

Default:

0

Special values:

0

Disables the lock because, in practice, the lockout period expires after 0 minutes.

2.70.5.13.6 Close destination

Specifies whether the firewall disconnects the source if the filter condition is true. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the **Port-block-list** under **Status** > **IPv6** > **Firewall**.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

No
Yes

Default:

No

2.70.5.13.7 Close time

Determines, for how many seconds the firewall closes the destination.

Console path:

Setup > **IPv6** > **Firewall** > **Trigger-Actions**

Possible values:

Max. 8 characters from `[0-9]`

Default:

0

Special values:

0

Disables the lock because, in practice, the lockout period expires after 0 minutes.

2.70.5.14 ICMP services

This table contains a list of ICMP-service.

Since ICMPv6 has central importance for numerous IPv6 features, basic ICMPv6 rules are already configured by default. You can not delete these rules.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.14.1 Name

Specifies the name of the ICMP service.

Console path:

Setup > **IPv6** > **Firewall** > **ICMP-Services**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.14.2 Type

Specifies the type of the ICMP service.

Lists with the official ICMP types and port codes are available in the Internet under *www.iana.org*.

Console path:

Setup > **IPv6** > **Firewall** > **ICMP-Services**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

2.70.5.14.3 Code

Specifies the codes of the ICMP service.

Lists with the official ICMP types and port codes are available in the Internet under *www.iana.org*.

Console path:

Setup > **IPv6** > **Firewall** > **ICMP-Services**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

2.70.5.15 Inbound rules

This table contains the rules that the firewall will apply to inbound connections.

The factory settings provide various rules for the most important applications.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.15.1 Name

Specifies the name of the inbound rule.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.5.15.2 Operating

This option enables the inbound rule.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

No
Yes

Default:

Yes

2.70.5.15.3 Prio

This information determines the priority with which the firewall applies the rule. A higher value determines a higher priority.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

2.70.5.15.5 Action

Specifies the action that the firewall performs if the rule condition is true. There are certain standard actions already specified in the table **Setup IPv** > **IPv6** > **Firewall** > **Actions**. In addition, you can also define your own actions.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

REJECT

2.70.5.15.7 Services

This information determines for which services the firewall applies this rule. There are certain services already specified in the table **Setup** > **IPv6** > **Firewall** > **Actions**. In addition, you can also define your own services.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

ANY

2.70.5.15.8 Source stations

This information determines for which source stations the firewall applies this rule. There are certain stations already specified in the table **Setup** > **IPv6** > **Firewall** > **Stations**. In addition, you can also define your own stations.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

ANYHOST

2.70.5.15.10 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.70.5.15.11 Src-Tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received. This can be used to restrict firewall rules to certain ARF contexts.

Console path:

Setup > **IPv6** > **Firewall** > **Inbound-Rules**

Possible values:

0 … 65535

Default:

0

Special values:

65535

The firewall rule is applied if the expected interface- or routing tag is 0.

65534

The firewall rule is applied if the expected interface- or routing tag is 1...65534.

0

Wildcard. The firewall rule is applied to all ARF contexts (the expected interface- or routing tag is 0...65535).

2.70.5.20 Allow-Route-Options

With this setting you specify whether the IPv6 firewall should allow or refuse routing options. The refusal of routing options always initiates a message about an IDS event. This action is independent of the settings in the IDS itself.

Console path:

Setup > **IPv6** > **Firewall**

Possible values:

No
Yes

Default:

No

2.70.5.21 Destination-Cache-Limit

This setting limits the number of "unanswered" destination cache entries. This number represents the number of destination addresses that do not respond during the *destination cache timeout*; once this number is exceeded, the firewall blocks any further **new** destination addresses for this interface. With the default setting (see below), this can happen if too many users on the LAN send requests to unreachable servers on the Internet.

Entering `0` as the limit globally disables the destination cache check for all interfaces. To disable the check for a particular interface, switch off the firewall on that interface. With the default setting (LAN: Firewall off // WAN: Firewall on) the device does not check the traffic of users within the LAN.

The default value is set high enough to avoid triggering the IDS during normal operation.

Console path:

Setup > **IPv6** > **Firewall**

Possible values:

0 … 99999

Default:

300

2.70.5.25 DSCP-support

If you set this parameter to Yes, then the DiffServ field in the IPv6-packet header is observed and evaluated as follows:

- **CSx (including CS0 = BE)**: Normal transmission
- **AFxx**: Secure transmission
- **EF**: Preferred transmission

Console path:

Setup > **IPv6** > **Firewall**

Possible values:

No
Yes

Default:

No

2.70.5.30 NPTV6

NPTv6 (Network Prefix Translation) according to *RFC 6296* allows the translation of one IPv6 prefix to another IPv6 prefix. The translation is 1:1, in that an address from prefix A is mapped to an address from prefix B. Only the prefix part is translated, the host part is retained. This method thus works "stateless". NPTv6 cannot be used to mask an entire network behind a single address, as with IPv4.

Application scenarios for NPTv6 are, for example, VPNs or networks with dynamic prefixes that should be reachable whatever the public address. If the provider assigns a dynamic prefix, the prefix usually changes every time a connection is established. This is not desirable if certain resources require fixed IP addresses. With NPTv6, addresses from the (private) ULA range fd00::/8 are then assigned to the clients in the network and an NPTv6 rule maps these addresses to the provider prefix.

Another use case is a load balancer scenario with several Internet providers, with each provider assigning its own prefix. With NPTv6, addresses from the ULA range fd00::/8 are assigned to the clients in the network and a number of NPTv6 rules map these addresses to the provider prefixes.

The IPv6 firewall must be enabled for NPTv6.

Console path:

Setup > **IPv6** > **Firewall**

2.70.5.30.1 Interface name

Name of the network or the peer on which NPTv6 is to be performed. If a prefix is to be mapped for a dynamic provider prefix, the name of the Internet connection or peer has to be configured here, e.g. INTERNET.

Console path:

Setup > **IPv6** > **Firewall** > **NPTV6**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.70.5.30.2 source-prefix

Source network prefix, e.g. an explicit prefix fd00::/64.

Console path:

Setup > **IPv6** > **Firewall** > **NPTV6**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

2.70.5.30.3 mapped-prefix

Prefix that the source prefix is mapped to. Here you can configure either an explicit prefix such as 2001:db8::/32, or the placeholder :: with the appropriate prefix length in the case that the provider assigns a dynamic prefix.

Console path:

Setup > **IPv6** > **Firewall** > **NPTV6**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

2.70.6 LAN interfaces

This table contains the settings for the LAN interfaces.

Console path:

Setup > **IPv6**

2.70.6.1 Interface name

Enter a name for the logical IPv6 interface that is defined by the physical interface (interface assignment) and the VLAN ID.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.6.2 Interface-ID

From the available physical interfaces, select the physical interface that combines with the VLAN ID to form the logical IPv6 interface.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

2.70.6.3 VLAN-ID

Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.

If you enter an invalid VLAN ID here, no communication will take place.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

0 … 4096

Default:

0

2.70.6.4 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

0 … 65535

Default:

0

2.70.6.5 Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

If the device sends router advertisements from this interface, it does not generate any IPv6 addresses even with auto-configuration enabled.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.6.6 Accept-RA

Enables or disables the processing of received router advertisement messages.

With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.6.7 Interface status

Enables or disables this interface.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

Down
Up

Default:

Up

2.70.6.8 Forwarding

Enables or disables the forwarding of data packets to other interfaces.

With forwarding disabled, no router advertisements are transmitted from this interface.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.6.9 MTU

Specify the applicable MTU for this interface.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

0 … 9999

Default:

1500

2.70.6.10 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

No

2.70.6.11 Comment

Enter a descriptive comment for this entry.

Entering a comment is optional.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.6.12 DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way the device avoids address conflicts on the network.

This option specifies the number of times that the device attempts to find duplicate IPv6 addresses on the network.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

0 … 9

Default:

1

2.70.6.13 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 LAN interface is started.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

Max. 1 characters from `[0-9]`

Default:

3

2.70.6.14 ND-Proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

No

2.70.6.15 Identifier-Mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

EUI-64

2.70.7 WAN interfaces

This table contains profiles for the settings of the WAN interfaces, which can be referenced in the **IPv6** column of various remote-site tables.

Console path:

Setup > **IPv6**

2.70.7.1 Interface name

Give a name to the IPv6 WAN-interface profile here. This name is used at the remote site to reference this profile in the column **IPv6**. It is preset with a default entry. This is selected automatically if nothing is explicitly specified at the remote site. Leaving this entry blank causes IPv6 to be disabled for this interface.

An entry in the WAN interfaces table can be referenced multiple times by remote sites.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

2.70.7.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

0 … 65534

Default:

0

2.70.7.3 Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

If the device sends router advertisements from this interface, it does not generate any addresses even with auto-configuration enabled.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.7.4 Accept-RA

Enables or disables the processing of received router advertisement messages.

With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.7.5 Interface status

Enables or disables this interface.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Down
Up

Default:

Up

2.70.7.6 Forwarding

Enables or disables the forwarding of data packets to other interfaces.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.7.7 Firewall

Enables the firewall for this interface.

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

No
Yes

Default:

Yes

2.70.7.8 Comment

Enter a descriptive comment for this entry.

Entering a comment is optional.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.7.9 DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way the device avoids address conflicts on the network.

This option specifies the number of times that the device attempts to find duplicate IPv6 addresses on the network.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 1 characters from `[0-9]`

Default:

1

2.70.7.10 PD-Mode

Mobile/cellular networks that support IPv6 only support DHCPv6 prefix delegation as of 3GPP Release 10. Consequently, a terminal device in a mobile network older than Release 10 can only be assigned one /64 prefix, for example by means of router advertisements. IPv6 support is easy to implement for smartphones or laptops using this method. However, an IPv6 router needs at least one more prefix that it can propagate to clients on the LAN.

IPv6 prefix delegation from the WWAN to the LAN allows clients to work on the LAN with a /64 prefix that is assigned from the WAN. A consequence of this is that a router is able to operate in an IPv6 cellular network without DHCPv6 prefix delegation and neighbor discovery proxy (ND proxy). The router announces the retrieved /64 prefix on the LAN by router advertisement, instead of adding it at the WAN interface. Clients generate an address from this prefix and use it for their IPv6 communications.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

DHCPv6

Prefix delegation is performed via DHCPv6.

Router-Advertisement

Prefix delegation is performed via router advertisement and the DHCPv6 client does not start.

Default:

DHCPv6

2.70.7.11 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 WAN interface is started.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 1 characters from `[0-9]`

Default:

3

2.70.7.13 Identifier-Mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable-Privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Default:

EUI-64

2.70.10 Operating

Switches the IPv6 stack on or off, globally. With the IPv6 stack deactivated, the device does not perform any IPv6-related functions.

Console path:

Setup > **IPv6**

Possible values:

No
Yes

Default:

No

2.70.11 Forwarding

If forwarding is turned off, the device transmits no data packets between IPv6 interfaces.

Forwarding is essential if you wish to operate the device as a router.

Console path:

Setup > **IPv6**

Possible values:

No
Yes

Default:

Yes

2.70.12 Router

These are the router settings.

Console path:

Setup > **IPv6**

2.70.12.1 Routing table

The table contains the entries to be used for routing packets with IPv6 addresses.

Console path:

Setup > **IPv6** > **Router**

2.70.12.1.1 Prefix

This prefix denotes the network range from which the current remote site, e.g. 2001:db8::/32, is to receive data

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]/:`

Default:

empty

2.70.12.1.2 Routing tag

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.

Routing tags are only necessary if used in combination with routing tags as set by firewall rules or as set at an interface.

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.70.12.1.3 Peer-or-IPv6

This is where you specify the remote site for this route. Enter one of the following options:

- An interface name
- An IPv6 address (e.g. 2001:db8::1)
- An interface supplemented with a link-local address (e.g. fe80::1%INTERNET)

The device stores the remote sites for IPv6 routing as (*WAN interfaces*).

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

Max. 56 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.12.1.4 Comment

Enter a descriptive comment for this entry.

Entering a comment is optional.

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.12.1.5 Admin-Distance

Administrative distance of this route. This parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. The default is 0, i.e. the value is assigned automatically by the operating system.

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

0 … 255

Default:

0

2.70.12.1.6 Active

Activates or deactivates this entry in the routing table.

Console path:

Setup > **IPv6** > **Router** > **Routing-Table**

Possible values:

Yes
No

Default:

Yes

2.70.12.2 Dest.-Cache-Timeout

The 'destination cache timeout' specifies how long the device remembers the path to a destination address when no packets are sent to it.

This value also influences the length of time the device takes to change the settings of the firewall: It accepts state changes after at least half of the 'destination cache timeout' time, on average after one quarter of the timeout. Thus with the default setting of 30 seconds, changes to the firewall come into effect on average after 7.5 seconds, but no later than after 15 seconds.

Console path:

Setup > **IPv6** > **Router**

Possible values:

0 … 999

Default:

30

2.70.13 ICMPv6

This menu contains the settings for ICMPv6.

Console path:

Setup > **IPv6**

2.70.13.1 Interface name

From the list of LAN/WAN interfaces defined in the device, specify the name of the interface for which you want to configure ICMPv6. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.70.13.2 Error bandwidth

With this setting you define the bandwidth (in kbps) which is available to the ICMPv6 protocol for sending error messages. Reduce this value in order to reduce the network load due to ICMPv6 messages.

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

0 … 99999

Default:

1000

2.70.13.3 Redirects

You enable or disable ICMP redirects with this setting. ICMP IPv6 neighbor redirect messages make it possible for the device to inform its hosts about a destination address by using a more direct path (e.g., the shorter one, measured by the number of hops).

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

Deactivating an
Activating the

Default:

Activating the

2.70.13.4 Refresh amount

Specifies the number of tokens added to the bucket in each interval before it is completely full.

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

0 … 65535

2.70.13.5 Interval

Sets the length of the interval in ms.

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

0 … 65535

2.70.13.6 Mode

Specifies the mode of the limitation.

Console path:

Setup > **IPv6** > **ICMPv6**

Possible values:

Bandwidth

Each packet to be sent is checked for whether the number of tokens in the bucket exceeds the size of the packet in kbit. If this is the case, the packet is sent and the corresponding number of tokens is removed from the bucket. Otherwise the packet is not sent.

Packets

Each packet to be sent is checked for whether at least one token is currently available in the token bucket. If this is the case, the packet is sent and a token is removed from the bucket. Otherwise the packet is not sent.

Disabled

No limitation, the packets are always sent.

2.70.14 RAS interface

In this directory, you specify the settings for RAS access via IPv6.

Console path:

Setup > **IPv6**

2.70.14.1 Interface name

Here you define the name of the RAS interface that the IPv6 remote sites use for access.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.14.2 Rtg-Tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will contain this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

Max. 5 characters from `0123456789`

Default:

0

2.70.14.3 Interface status

Enable or disable this interface here.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

Operating
Idle

Default:

Operating

2.70.14.4 Forwarding

Enables or disables the forwarding of data packets to other interfaces.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

Yes
No

Default:

Yes

2.70.14.5 Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, change the setting under **IPv6** > **Firewall** > **Enabled** to **yes**.

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

Yes
No

Default:

Yes

2.70.14.6 DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way the device avoids address conflicts on the network.

This option specifies the number of times that the device attempts to find duplicate IPv6 addresses on the network.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

1 characters from `0123456789`

Default:

0

2.70.14.7 Remote site

Specify the remote site or a list of remote sites for RAS dial-in users.

The following values are possible:

- An individual remote site from the table under **Setup** > **WAN** > **PPTP-Peers** or **SetupPPPoE-Server** > **Name-List**.
- The wildcard "*" makes the interface valid for all PPTP and PPPoE peers.
- The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL" .

By using wildcards you can implement template interfaces, which apply to peers which are named accordingly. In this manner, the name of the IPv6 RAS interface can be used many places in the IPv6 configuration.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.70.14.8 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **IPv6** > **RAS-Interface**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.15 Polling-Table

In this table, specify the settings for the ICMPv6 polling. As with LCP monitoring or ICMP polling for IPv4, ICMPv6 polling regularly sends requests to a remote peer. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMPv6 pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in this table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IPv6 addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IPv6 addresses are unavailable is the connection considered to have failed.

Console path:

Setup > **IPv6**

2.70.15.1 Peer

Here you enter the name of a peer from the list of remote sites.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.15.2 IPv6-Address-1

Enter here the first of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.70.15.3 IPv6-Address-2

Enter here the second of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.70.15.4 IPv6-Address-3

Enter here the third of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.70.15.5 IPv6-Address-4

Enter here the fourth of up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.70.15.6 Time

Enter the ping interval in seconds here.

If you enter 0 both here and at *2.70.15.7 Try* on page 1636, a default interval of 20 seconds and 5 repetitions is used.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.70.15.7 Try

Enter the number of tries each second if no response is received to a ping. If the repeated pings also go unanswered, the connection is terminated.

If you enter 0 both here and at *2.70.15.6 Time* on page 1635, a default interval of 20 seconds and 5 repetitions is used.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.70.15.8 Loopback-Addr.

This is where you can configure an optional sender address to be used instead of the one that would normally be selected automatically for this target address.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.70.15.9 Type

This setting influences the behavior of the polling.

Console path:

Setup > **IPv6** > **Polling-Table**

Possible values:

Auto

The device only polls actively if it receives no data. ICMP packets received are not considered to be data and are still ignored.

Forced

The device polls in the given interval.

Default:

Auto

2.70.16 NDP

This menu allows you to find the settings for the ND cache.

Console path:

Setup > **IPv6**

2.70.16.1 Global-Cache-Limit

Specifies the maximum allowed number of IPv6 neighbor cache entries per device.

Console path:

Setup > **IPv6** > **NDP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

20000

2.70.16.2 Cache-Limit-Per-Interface

Specifies the maximum allowed number of IPv6 neighbor cache entries per interface.

Console path:

Setup > **IPv6** > **NDP**

Possible values:

Max. 10 characters from `[0-9]`

Default:

10000

2.70.16.3 NDP-Bridge-Optimization

Switch for optimizing bridge negotiations for IPv6 and the Neighbor Discovery Protocol (NDP).

Console path:

Setup > **IPv6** > **NDP**

Possible values:

No

For a packet received on a bridge link, the Neighbor Discovery stores the bridge information only. The switch port is set to 0. This forces the bridge to perform a MAC address lookup to find the actual link (and switch port).

Yes

The Neighbor Discovery stores the LAN information and switch port of the received neighbor solicitation/advertisement in the neighbor cache, regardless of whether the packet was received on a bridge link.

Default:

Yes

2.71 IEEE802.11u

The tables and parameters in this menu are used to make all settings for connections according to IEEE 802.11u and Hotspot 2.0.

Console path:

Setup

2.71.1 ANQP profiles

Using this table you manage the profile lists for IEEE802.11u or ANQP. IEEE802.11u profiles give you the ability to group certain ANQP elements and to assign them to mutually independent logical WLAN interfaces in the table **Setup** > **Interfaces** > **WLAN** > **IEEE802.11u** under **IEEE802.11u-Profile**. These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.

Console path:

Setup > **IEEE802.11u**

2.71.1.1 Name

Assign a name for the ANQP 2.0 profile here. You specify this name later in the table **Setup** > **Interfaces** > **WLAN** > **IEEE802.11u** under **ANQP-Profile**.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.2 Include-in-Beacon-OUI

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional-OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

Multiple OIs can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.3 Additional-OUI

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

Multiple OIs can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.4 Domain list

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

Multiple domains can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.5 NAI realm list

Enter a valid NAI realm profile in this field.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.6 Cellular list

Enter a valid cellular network profile in this field.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.1.6 Network-Auth-Type-List

Enter one or more valid authentication parameters in this field.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **ANQP-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.3 Venue name

In this table, enter general information about the location of the access point.

In the event of a manual search, additional details on the Venue information help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

Console path:

Setup > **IEEE802.11u**

2.71.3.1 Name

Use this parameter to enter a name for the list entry in the table.

On a standalone access point, LCOS overwrites custom names with `VENUE` because a single access point can only be on one site.

Console path:

Setup > **IEEE802.11u** > **Venue-Name**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.3.2 Venue name

Enter a short description of the location of your device for the selected language.

Console path:

Setup > **IEEE802.11u** > **Venue-Name**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.3.2 Language

Select the language in which you store information about the location.

Console path:

Setup > **IEEE802.11u** > **Venue-Name**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian

Default:

None

2.71.4 Cellular-Network-Information-List

Using this table, you manage the profile lists for the cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.

In the setup menu you assign an ANQP profile to this list by using the table **ANQP-Profiles**.

Console path:

Setup > **IEEE802.11u**

2.71.4.1 Name

Assign a name for the cellular network profile, such as an abbreviation of the network operator in combination with the cellular network standard used. You specify this name later in the table **Setup** > **IEEE802.11u** > **ANQP-Profiles** under **Cellular-List**.

Console path:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.4.2 Country code

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.

Console path:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.71.4.3 Network code

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Console path:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Possible values:

Max. 32 characters from `[0-9]`

Default:

empty

2.71.5 Network-Authentication-Type

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

Console path:

Setup > **IEEE802.11u**

2.71.5.1 Network-Auth-Type

Choose the context from the list, which applies before forwarding.

Console path:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Accept-Terms-Cond
An additional authentication step is set up that requires the user to accept the terms of use.

Online-Enrollment
An additional authentication step is set up that requires the user to register online first.

Http-Redirection
An additional authentication step is set up to which the user is forwarded via HTTP.

DNS-Redirection
An additional authentication step is set up to which the user is forwarded via DNS.

Default:

Accept-Terms-Cond

2.71.5.2 Redirect URL

Enter the address to which the device forwards stations for additional authentication.

Console path:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.5.3 Name

Assign a name for the table entry, e.g., `Accept Terms and Conditions`.

Console path:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.6 ANQP-General

The general settings for ANQP are made in this menu.

Console path:

Setup > **IEEE802.11u**

2.71.6.1 Venue group

The venue group describes the environment where you set up the access point. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

Console path:

Setup > **IEEE802.11u** > **ANQP-General**

Possible values:

Unspecified
Unspecified
Assembly
Assembly
Business
Business
Educational
Educational:
Factory-and-Industrial
Factory and industry
Institutional
Institutional
Mercantile
Mercantile
Residential
Halls of residence
Storage
Warehouse
Utility and miscellaneous
Utility and miscellaneous

Vehicular
Vehicular
Outdoor
Outdoor

Default:

Unspecified

2.71.6.2 Venue type

Using the location type code (venue type), you have the option to specify details for the location group. These values are also specified by the standard. The possible type codes can be found in the following table.

The default value for each is "0".

Table 20: Overview of possible values for venue groups and types

Venue group	Code = Venue-Type-Code
Unspecified	
Assembly	› 0 = unspecified assembly › 1 = stage › 2 = stadium › 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) › 4 = amphitheater › 5 = amusement park › 6 = place of worship › 7 = convention center › 8 = library › 9 = museum › 10 = restaurant › 11 = theater › 12 = bar › 13 = café › 14 = zoo, aquarium › 15 = emergency control center
Business	› 0 = unspecified business › 1 = doctor's office › 2 = bank › 3 = fire station › 4 = police station › 6 = post office › 7 = office › 8 = research facility › 9 = law firm
Educational:	› 0 = unspecified education

Venue group	Code = Venue-Type-Code
	› 1 = primary school › 2 = secondary school › 3 = college
Factory and industry	› 0 = unspecified factory and industry › 1 = factory
Institutional	› 0 = unspecified institution › 1 = hospital › 2 = long-term care facility (e.g., nursing home, hospice) › 3 = rehabilitation clinic › 4 = organizational association › 5 = prison
Mercantile	› 0 = unspecified commerce › 1 = retail store › 2 = food store › 3 = Automobile workshop › 4 = shopping center › 5 = gas station
Halls of residence	› 0 = unspecified residence hall › 1 = private residence › 2 = hotel or motel › 3 = student housing › 4 = guesthouse
Warehouse	› 0 = unspecified warehouse
Utility and miscellaneous	› 0 = unspecified service and miscellaneous
Vehicular	› 0 = unspecified vehicle › 1 = passenger or transport vehicles › 2 = aircraft › 3 = bus › 4 = ferry › 5 = ship or boat › 6 = train › 7 = motorcycle
Outdoor	› 0 = unspecified outdoor › 1 = Municipal WLAN network › 2 = city park › 3 = rest area › 4 = traffic control › 5 = bus stop › 6 = kiosk

Console path:

Setup > **IEEE802.11u** > **ANQP-General**

2.71.6.5 IPv4-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv4.

Console path:

Setup > **IEEE802.11u** > **ANQP-General**

Possible values:

Not-Available
IPv4 address type is not available.

Public-Addr-Available
Public IPv4 address is available.

Port-Restr-Addr-Avail
Port-restricted IPv4 address is available.

Single-Nat-Priv-Addr-Avail
Private, single NAT-masked IPv4 address is available.

Double-Nat-Priv-Addr-Avail
Private, double NAT-masked IPv4 address is available.

Port-Restr-Single-Nat-Addr-Avail
Port-restricted IPv4 address and single NAT-masked IPv4 address is available.

Port-Restr-Double-Nat-Addr-Avail
Port-restricted IPv4 address and double NAT-masked IPv4 address is available.

Availability-not-known
The availability of an IPv4 address type is unknown.

Storage
Warehouse

Utility and miscellaneous
Utility and miscellaneous

Vehicular
Vehicular

Outdoor
Outdoor

Default:

Single-Nat-Priv-Addr-Avail

2.71.6.6 IPv6-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv6.

Console path:

Setup > **IEEE802.11u** > **ANQP-General**

Possible values:

Not-Available
IPv6 address type is not available.

Available
IPv6 address type is available.

Availability-not-known
The availability of an IPv6 address type is unknown.

Default:

Not-Available

2.71.7 Hotspot2.0

The general settings for Hotspot 2.0 are made in this menu.

Console path:

Setup > **IEEE802.11u**

2.71.7.1 Operator list

Using this table you manage the cleartext name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.1.1 Name

Assign a name for the entry, such as an index number or combination of operator-name and language.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.7.1.2 Operator name

Enter the cleartext name of the hotspot operator.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.7.1.4 Language

Select a language for the hotspot operator from the list.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian

Default:

None

2.71.7.2 Connection capability

This table contains a set list of the connection capabilities that you referenced as a comma-separated list in the table **Hotspot2.0-Profiles** in the input field **Connection-Capabilities**. Possible status values for each of these services are 'closed' (**-C**), 'open' (**-O**) or 'unknown' (**-U**).

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.2.4 Name

This entry displays the name of the connection capability that you referenced as a comma-separated list in the table **Hotspot2.0-Profiles** in the input field **Connection-Capabilities**.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Connection-Capability**

2.71.7.4 Link status

Using this entry, you specify the connectivity status of your device to the Internet.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

Possible values:

Auto
The device determines the status value for this parameter automatically

Link-Up
The connection to the Internet is established.

Link-Down
The connection to the Internet is interrupted.

Link-Test
The connection to the Internet is being established or is being checked.

Default:

Auto

2.71.7.7 Downlink speed

Using this entry, you enter the nominal value for the maximum receiving bandwidth (downlink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

Possible values:

0 … 4294967295 Kbps

Default:

0

2.71.7.8 Uplink-Speed

Using this entry you can enter the nominal value for the maximum transmission bandwidth (uplink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

Possible values:

0 … 4294967295 Kbps

Default:

0

2.71.7.9 Hotspot2.0-Profiles

Using this table you manage the profile lists for the Hotspot 2.0. Hotspot-2.0 profiles allow you to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign logical WLAN interfaces in the table **Setup** > **Interfaces** > **WLAN** > **IEEE802.11u** under **HS20-Profile**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.9.1 Name

Assign a name for the Hotspot 2.0 profile here. You specify this name later in the table **Setup** > **Interfaces** > **WLAN** > **IEEE802.11u** under **HS20-Profile**.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.7.9.2 Operator name

Enter a valid profile for hotspot operators in this field.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.71.7.9.3 Connection capabilities

Enter one or more valid entries for the connection capabilities in this field. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown".

Specify a name from the table **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Connection-Capability**.

Multiple names can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.71.7.9.4 Operating class

Enter the code for the global operating class of the access point. The operating class is used to inform a station about the frequency bands and channels used by your access point. Example:

`81`

Operation at 2.4 GHz with channels 1-13

`116`

Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at *standards.ieee.org*.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[0-9],`

Default:

empty

2.71.7.9.5 Hotspot2.0-Release

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Release-1
Release-2

2.71.7.9.6 Domain-Id

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16-bit value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.71.7.9.7 OSU-Network-Name

Name of the SSID that provides access to the OSU server.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.71.7.9.8 OSU-Providers

List of OSU provider names in *2.71.7.10 OSU-Providers* on page 1655 that are supported in the profile.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profiles**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.71.7.10 OSU-Providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.10.1 Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.71.7.10.2 Language

Set the language supported by this OSU provider.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian
Korean

2.71.7.10.3 Friendly-Name

Give this OSU provider a descriptive name.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.71.7.10.4 OSU-Methods

Set the OSU methods used by this OSU provider. See also *2.71.7.11 OSU-Methods* on page 1658. Options are “OMA-DM” or “SOAP-XML-SPP”.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.71.7.10.5 URI

Enter a URI where a client can reach the OSU server.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.71.7.10.6 NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.71.7.10.7 Service-Description

Enter a descriptive text for this service here.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.71.7.10.8 Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the **File management** feature. We recommend PNG as the file format.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

None
OSU-Prov-Img-1
OSU-Prov-Img-2
OSU-Prov-Img-3
OSU-Prov-Img-4
OSU-Prov-Img-5
OSU-Prov-Img-6
OSU-Prov-Img-7
OSU-Prov-Img-8
OSU-Prov-Img-9
OSU-Prov-Img-10
OSU-Prov-Img-11
OSU-Prov-Img-12
OSU-Prov-Img-13
OSU-Prov-Img-14
OSU-Prov-Img-15
OSU-Prov-Img-16

2.71.7.10.9 Icon-Language

This item sets the language for the selected icon.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0** > **OSU-Providers**

Possible values:

None
English
German
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabic
Korean

2.71.7.11 OSU-Methods

This table contains a fixed list of methods available on the online sign-up server when using Passpoint® Release 2.

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.12 Load-Meas.-Duration

Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

Console path:

Setup > **IEEE802.11u** > **Hotspot2.0**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.71.8 Auth parameter

This table contains a set list of possible authentication parameters for the NAI realms. You reference this list in the table **NAI-Realms** as a comma-separated list in the input field **Auth-Parameter**.

Table 21: Overview of possible authentication parameters

Parameter	Sub-Parameter	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password
	None	No credentials required
TunnelEAPCredentials.*		
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Console path:

Setup > **IEEE802.11u**

2.71.8.1 Name

This entry displays the name of the authentication parameters that you referenced as a comma-separated list in the table **NAI-Realms** in the input field **Auth-Parameter**.

Console path:

Setup > **IEEE802.11u** > **Auth-Parameter**

2.71.9 NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.

In the setup menu you assign an ANQP profile to this list by using the table **ANQP-Profiles**.

Console path:

Setup > **IEEE802.11u**

2.71.9.1 Name

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. You specify this name later in the table **Setup** > **IEEE802.11u** > **ANQP-Profiles** under **NAI-Realm-List**.

Console path:

Setup > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.9.2 NAI realm

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest case, is `<username>@<realm>`, for `user746@providerX.org`, and therefore the corresponding realm is `providerX.org`.

Console path:

Setup > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.71.9.3 EAP method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication procedure

Console path:

Setup > **IEEE802.11u** > **NAI-Realms**

Possible values:

None

Select this setting when the relevant NAI realm does not require authentication.

EAP-TLS

Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate installed by the user.

EAP-SIM

Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.

EAP-TTLS

Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.

EAP-AKA

Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

Default:

None

EAP-TLS

2.71.9.4 Auth parameter

In this field, enter the appropriate authentication parameters for the EAP method using a comma-separated list, e.g., for EAP-TTLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` or for EAP-TLS `Credentials.Certificate`.

Select a name from the table **Setup** > **IEEE802.11u** > **Auth-Parameter**. Multiple names can be provided in a comma-separated list.

Console path:

Setup > **IEEE802.11u** > **NAI-Realms**

Possible values:

Max. 65 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.83 SMS

This menu contains the options for the SMS module, which performs the sending and receiving of text messages (SMS).

Console path:

Setup

2.83.1 SMSC address

This parameter allows you to configure an alternative number for the "short message service center" (SMSC).

By default, the device uses the phone number stored in the USIM card, which you can view by calling the status value **SMSC number** (SNMP ID 1.83.5). The SMS messages can be sent to a specific SMSC if you specify a different phone number.

Console path:

Setup > **SMS**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.83.2 Inbox limit

This parameter lets you set the maximum number of text messages stored in the device inbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry.

Console path:

Setup > **SMS**

Possible values:

0 … 999999

Default:

100

Special values:

0

This value disables the limit, i.e. an unlimited number of messages will be stored.

2.83.3 Outbox limit

This parameter lets you set the maximum number of text messages stored in the device outbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry.

Console path:

Setup > **SMS**

Possible values:

0 … 999999

Default:

100

Special values:

0

This value disables the limit, i.e. an unlimited number of messages will be stored.

2.83.4 Outbox preservation

This parameter is used to configure how the device handles SMS text messages.

Console path:

Setup > **SMS**

Possible values:

None

Sent messages are not saved.

All

Sent messages are saved permanently.

Default:

All

2.83.5 Mail-Forward-Addr.

This parameter sets an optional e-mail address to which the device will forward any incoming SMS text messages.

E-mail routing will only work if a valid SMTP account is configured in the device.

Console path:

Setup > **SMS**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.83.6 SMS-Forward-Addr.

This parameter gives you the option to set an SMS phone number to which the device will forward any incoming SMS text messages.

Please note that additional charges may apply for sending SMS text messages via connections that have been established.

Console path:

Setup > **SMS**

Possible values:

Max. 63 characters from `[0-9]-`

Default:

empty

2.83.7 SMS-Forward-Limit

This parameter allows you to limit the number of SMS text messages that can be forwarded. When this limit is reached, the device sends one final SMS text message informing the relevant phone number that the limit has been reached.

Console path:

Setup > **SMS**

Possible values:

0 … 999999

Default:

20

Special values:

0

This value disables the limit, i.e. an unlimited number of messages will be forwarded.

2.83.8 Syslog

Use this parameter to specify if and how the arrival of text messages is logged to the SYSLOG.

Console path:

Setup > **SMS**

Possible values:

No

Incoming text messages are not logged to SYSLOG.

SenderOnly

The arrival of a text message is recorded to the SYSLOG together with the sender's phone number.

Full

The arrival of a text message is recorded to the SYSLOG together with the sender's phone number and the message in full.

Default:

No

2.83.9 Max-Send-Attempts

Specify how many times the device attempts to send an SMS. Once the maximum number of send attempts is reached, the message remains in the outbox and the device generates an error message in the syslog.

Console path:

Setup > **SMS**

Possible values:

0 … 4294967295

Default:

2

Special values:

0

Unlimited attempts

2.83.10 Operating

Enables or disables sending and receiving of SMS text messages on the device.

Console path:

Setup > **SMS**

Possible values:

No

Sending and receiving SMS is disabled.

Yes

Sending and receiving SMS is enabled.

Default:

Yes

2.83.11 Action-Table

Use this table to react to incoming SMS text messages with predefined actions. This allows you to respond to an incoming SMS (e.g. data budget used up) by sending your own SMS to the Internet provider, for example to book a new data budget.

Console path:

Setup > **SMS**

2.83.11.1 Idx.

Index for this entry in the list.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 6 characters from `0123456789`

Default:

empty

2.83.11.2 Operating

Activates or deactivates this table entry.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

No

Disables the table entry.

Yes

Enables the table entry.

Default:

Yes

2.83.11.4 Sender

Sender address of the incoming SMS text message, which is the basis for the subsequent action. For example, 7277 for Deutsche Telekom.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.83.11.5 Check-For

Content of the incoming SMS text message to be checked for. For example, `contains=' used up'` in the event of an exhausted data budget. The text checks are case-sensitive!

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.83.11.6 Action

Defines the action to be executed after checking the specifications under *2.83.11.4 Sender* on page 1666 and *2.83.11.5 Check-For* on page 1667. For example, `exec:smssend -d 7277 -t "Speed"` to book a SpeedOn in the Deutsche Telekom network. With `exec` a command is executed on the command line, in this case the command `smssend`.

The possible commands correspond to those of the normal action table, see *2.2.25.6 Action* on page 87.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.83.11.7 Lock-Time

Defines the lockout time in seconds, in which the action may not be executed again.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 9 characters from `0123456789`

Default:

300

2.83.11.8 Syslog

Text field for defining the message to be written to the syslog when this action is executed.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.83.11.10 Comment

Comment field.

Console path:

Setup > **SMS** > **Action-Table**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.88 Wireless ePaper

Configure the settings for the Wireless ePaper module here.

Console path:

Setup

2.88.1 Operating

This entry allows you to set the operating mode of the module.

Console path:

Setup > **Wireless-ePaper**

Possible values:

Off

The module is not enabled.

Manual

Wireless ePaper configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Manual

2.88.2 Port

Assign a port to the Wireless ePaper module.

Console path:

Setup > **Wireless-ePaper**

Possible values:

Max. 5 characters from `[0-9]`

Default:

2002

2.88.3 Channel

Set which channel the Wireless ePaper module should use.

Console path:

Setup > **Wireless-ePaper**

Possible values:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:

2425MHz

2.88.4 Channel coordination

Prevents collisions on ePaper channels due to APs within range of each other.

Console path:

Setup > **Wireless-ePaper**

2.88.4.1 Operating

The coordinated channel selection is activated or deactivated here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0

No

1

Yes

Default:

1

2.88.4.2 Network

Here you specify the network that the access points are to use to communicate with each other.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

16 characters from the following character set `[A-Z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

2.88.4.3 Announce address

Set the announce address here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

39 characters from the following character set: `[0-9 A-F a-f :.]`

2.88.4.4 Announce port

Set the announce port here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.88.4.5 Announce interval

Set the announce interval here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.88.4.6 Announce timeout factor

Set the announce timeout factor here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.88.4.7 Announce timeout interval

Set the announce timeout interval here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.88.4.8 Announce master backoff interval

Set the announce master backoff interval here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

2.88.4.9 Coordination port

Set the coordination port here.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.88.4.10 Coordination keep-alive interval

Here you set the coordination keep-alive interval.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.88.4.11 Coordination reconnect interval

Here you set the coordination reconnect interval.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.88.4.12 Assignment switch threshold

Here you set the assignment switch threshold.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

2.88.4.13 Distance weighting

Here you set the weighting of WLAN distance.

A higher value means a better weighting.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

2.88.4.14 Channel weighting

Here you set the weighting of a preferred channel.

A higher value means a better weighting.

Console path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

2.93 Routing protocols

In this directory, you configure the routing protocols and the route monitor.

Console path:

Setup

2.93.1 BGP

This directory is used to configure the device for the Border Gateway Protocol version 4 (BGPv4).

Console path:

Setup > **Routing-protocols**

2.93.1.1 BGP instance

This table is used to configure the BGP instances.

Since the device only supports one BGP instance at a time, this table contains just one entry.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.1.1 Name

Contains the name of the BGP instance.

The factory settings already include the entry “DEFAULT”.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

2.93.1.1.2 Operating

Activates or deactivates this BGP instance

This setting only takes effect if BGP is activated on the device.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Yes

The BGP instance is enabled.

No

The BGP instance is disabled.

Default:

No

2.93.1.1.3 AS number

The AS number assigned to this BGP instance.

It is only possible to connect to a BGP router that does not support 32-bit AS numbers if you enter a 16-bit AS number here (less than 65536).

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.93.1.1.4 Router ID

The router ID (IPv4 address) of this particular BGP instance.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.93.1.1.5 Syslog

The device is able to store events, such as disconnects of neighbors associated with this BGP instance, to the SYSLOG. Use this option to enable or disable this feature.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Yes

Logging to SYSLOG is enabled.

No

Logging to SYSLOG is disabled.

Default:

No

2.93.1.1.6 Port

Here you specify the port used by the BGP instance to listen to incoming connections from neighbors.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 5 characters from `[0-9]`

Default:

179

2.93.1.1.7 Comment

Comment about this BGP instance.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

Default instance

2.93.1.1.8 Check-First-AS

Checks whether the first AS number in the AS path of received Update messages corresponds to the AS number of the neighbor. If this is not the case, this route is discarded.

This check must be disabled if the router is connected with a BGP route server which, although it distributes routes, is not itself in the routing path and/or inserts its own AS into the AS path.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Yes
No

Default:

Yes

2.93.1.1.9 AS-Path-Limit

Maximum number of permitted AS numbers in the AS path of received Update messages. If the limit is exceeded, the device discards the route. An AS-Path-Limit provides protection against messages from incorrectly configured routers that advertise AS paths that are too long.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.93.1.1.10 Cluster-ID

Cluster-ID of the router in case it is configured as a route reflector. This is entered as an IPv4 address.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Max. 15 characters from `[0-9]`

Default:

0.0.0.0

2.93.1.1.11 Route-Reflector

This specifies whether the router assumes the function of a route reflector.

When operating iBGP, all of the BGP routers usually need to be fully meshed, i.e. each BGP router must have established a BGP connection to every other BGP router. A route reflector negates this requirement and enables iBGP routers to form, for example, a star-shaped topology. A route reflector forwards the iBGP routes to all of the route-reflector clients.

A route reflector is able to serve route-reflector clients as well as normal BGP clients. In both cases no special configuration of the client is necessary.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Yes
No

Default:

No

2.93.1.1.12 TX-Loop-Detection

When activated, loop detection influences the behavior of the BGP instance as follows:

1. The BGP instance does not propagate any routes to neighbors, whose AS numbers are in the AS path of the route.
2. The BGP instance sends local routes to iBGP neighbors only if the neighbor is a route-reflector client and the local BGP instance is a route reflector.
3. The BGP instance does not distribute a route to neighbors who have already learned it.

These measures reduce the unnecessary sending of messages that a neighbor might reject due to its own loop detection.

In certain VPN/ARF scenarios, the TX-loop detection must be disabled.

Console path:

Setup > **Routing-Protocols** > **BGP** > **BGP-Instance**

Possible values:

Yes
No

Default:

Yes

2.93.1.2 Neighbors

This table is used to configure the BGP neighbors.

A new entry can be created here simply by specifying an **IP address**, although BGP instances will ignore this entry unless the following conditions are met:

- The entry is enabled by setting **Operating** to "Yes".
- The **Instance name** corresponds to the BGP instance name configured under **Setup** > **Routing-Protocols** > **BGP** > **BGP-Instance**.
- The **Neighbor profile** corresponds to a profile entered under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

The table is empty by default.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.2.1 IP-Address

Specifies this BGP neighbor's IP address (IPv4 or IPv6) as used by the device to establish a BGP connection in the "active" or "delayed" connection mode. When using a link-local IPv6 address, it must be specified with % and the name of the logical interface, e.g. "fe80::1%INTRANET".

This entry must match the IP address (e.g. physical interface address, loopback address) reported by this neighbor in an incoming connection.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 56 characters from `[A-F][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.1.2.2 Port

Shows the port on which the BGP neighbor expects inbound BGP messages and, correspondingly, the port used by the device for outbound connections of the connection type "active" or "delayed".

The device accepts incoming connections from any source port that is used by the sender.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 5 characters from `[0-9]`

Default:

179

2.93.1.2.3 Loopback address

Contains the sender address (IPv4 or IPv6) that the device uses when connecting to the BGP neighbor. The field allows you to enter loopback addresses as configured under **Setup** > **TCP-IP** > **Loopback-List** and **Setup** > **IPv6** > **Network** > **Loopback**.

Entry is optional and is only relevant for the connection modes "active" and "delayed".

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 56 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Special values:

empty

When setting the sender address for the TCP connection, the device attempts to find a suitable loopback address from the same subnet as the IP address of the BGP neighbor.

2.93.1.2.4 Rtg-Tag

Contains the routing tag. The device denies the connection if the routing tag does not match with the incoming connection.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65536

Default:

0

2.93.1.2.5 Remote AS

Contains the AS number of the BGP neighbor.

If the AS number of the BGP neighbor is identical to the AS number of the device's own BGP instance, then this neighbor is an iBGP peer (internal BGP) within the AS.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.93.1.2.6 Name

Contains the name of the BGP neighbor.

Use this name as an argument when executing the following actions:

› **Manual start** under **Setup** > **Routing-Protocols** > **BGP**

- **Manual stop** under **Setup** > **Routing-Protocols** > **BGP**
- **Active start** under **Setup** > **Routing-Protocols** > **BGP**

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.2.7 Operating

Activates or deactivates this BGP neighbor.

The activation of the BGP neighbor triggers the establishment of a BGP connection, if applicable.

Outbound and inbound connections are not possible with a disabled BGP neighbor.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Yes

The BGP neighbor is enabled. It is possible to establish a BGP connection with it.

No

The BGP neighbor is disabled. It is not possible to establish a BGP connection (transmit or receive) with it.

Default:

Yes

2.93.1.2.8 Password

The device and the BGP neighbor authenticate themselves by exchanging this password in the form of an MD5 signature in the TCP packets.

Authentication is not used if no password is set.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.93.1.2.9 Neighbor profile

Contains the name of the BGP neighbor profile from **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

DEFAULT

2.93.1.2.10 Connection mode

Sets the mode in which the connection is established from the device to this BGP neighbor.

All three modes accept connections initiated by the neighbor.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Operating

In this mode the device attempts to connect to the BGP neighbor as soon as, among other things, one of the following conditions is met:

- The BGP neighbor is completely configured.
- You execute the action **Manual start**.
- You start the device.
- The BGP instance is enabled under **Setup** > **Routing-Protocols** > **BGP** > **BGP-Instance** > **Operating**.
- You enable this BGP neighbor under **Operating**.

If the connection cannot be established actively, it will be tried again after 120 seconds.

Passive

In this mode the device does not actively connect to the BGP neighbor; instead, it waits for a connection request from the BGP neighbor.

Delayed

In this mode the device waits for a timeout before it tries to connect to the BGP neighbor. The conditions for establishing a connection are the same as for the "Active" mode.

The delay time is set under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** > **Connection-Delay**

Default:

Operating

2.93.1.2.11 Connection-Delay

Specifies the wait time in seconds that the device waits in the connection type "delayed" whether a connection is established from the remote side. A connection to this BGP neighbour is then actively established.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 5 characters from `[0-9]`

Default:

120

2.93.1.2.12 Instance name

Specifies the name of the associated BGP instance under **Setup** > **Routing-Protocols** > **BGP** > **BGP-Instance**.

If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

DEFAULT

2.93.1.2.13 Inbound policy

Specifies the policy used by the device to filter the incoming prefixes from this BGP neighbor.

The policy is configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters**.

If you leave this field empty, the device filters the incoming prefixes according to the default policy under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Default**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.2.14 Outbound policy

Specifies the policy used by the device to filter the outbound prefixes to this BGP neighbor.

The policy is configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters**.

If you leave this field empty, the device filters the outbound prefixes according to the default policy under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Default**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.2.15 Comment

Contains a comment about this BGP neighbor.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.2.16 Route-Reflector-Client

Specifies whether this neighbor is treated as a route-reflector client, in which case the device reflects iBGP routes back to it.

This switch is valid only if

- The device has been configured as a route reflector in the in the BGP instance, i.e. is a route reflector itself, or
- The remote AS number matches its own AS number (iBGP).

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Yes
No

Default:

No

2.93.1.2.17 BFD-Profile

Contains the name of a BFD profile from **Setup** > **Routing-Protocols** > **BFD** > **Profiles**. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

2.93.1.3 Neighbor profiles

This table is used to configure the BGP neighbor profiles.

Neighbor profiles are used to specify a general configuration, which can be assigned to different BGP neighbors.

A default entry already exists under the name “DEFAULT” and containing the comment “Default Entry”.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.3.1 Name

Contains the name of the profile.

This name is used in the following tables, among other things:

- **Neighbor profile** under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**
- **Neighbor profile** under **Setup** > **Routing-Protocols** > **BGP** > **Address-Family** > **IPv4**
- **Neighbor profile** under **Setup** > **Routing-Protocols** > **BGP** > **Address-Family** > **IPv6**

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.3.2 Route update delay

This is the minimum delay in seconds between BGP advertisements sent by the device to neighbors using this profile.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

30

2.93.1.3.3 Send-TTL

Specifies the TTL (time to live) that the device sets for TCP packets sent to the BGP neighbors that use this profile.

For directly connected neighbors, this value is set to "1". For eBGP environments, you can increase this value by 1 per hop.

For iBGP sessions, the device ignores this value and defaults to the maximum TTL value.

This value must be "0" if **Recv-TTL** is set to a value other than "0". The device automatically uses the value "1" if both **Send-TTL** and **Recv-TTL** are set to "0".

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

2.93.1.3.4 Recv-TTL

Specifies the minimum TTL (time to live) required of inbound TCP packets from BGP neighbors that use this profile. Inbound TCP packets must have a TTL greater than or equal to this value in order to be accepted.

The device ignores this value in iBGP sessions.

If this value is not equal to "0", the device sets the internal value for **Send-TTL** to "255".

This value must be "0" if **Send-TTL** is set to a value other than "0".

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

Special values:

0

Disables TTL checks of inbound TCP packets.

2.93.1.3.5 Keepalive

Specifies the time in seconds for the keepalive timer. After this time has elapsed, the device sends a keepalive message to the neighbors using this profile in order to keep the BGP connection intact.

The device should send at least three keepalive messages per unit of holdtime. For this reason the value should be max. one third of the holdtime. If the value is set higher than this or equal to "0", the LCOS automatically sets an internal value that is one-third of the holdtime.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

30

0 … 65536

2.93.1.3.6 Holdtime

If the router does not receive regular BGP keepalive, update or notification messages within the configured BGP short-hold time, the router will terminate the BGP session and send a notification with the error code "Hold Timer Expired".

The device negotiates this value with the BGP neighbors during connection establishment. The lower of the two values is considered to be valid.

If negotiation results in a value of "0", the device considers the connection to be valid until it receives a connection error or the connection breaks. No keepalive messages are sent to the BGP neighbors during this period, even if the keepalive timer is set with a value.

In accordance with the RFC, the values "1" and "2" are not permitted.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

90

Special values:

0

The device considers the connection to be valid until an error notification is received or the connection breaks. The transmission of keepalive messages is deactivated even if the keepalive timer is set with a value.

2.93.1.3.7 Filter private AS

Controls the removal/replacement of private AS entries (64512 – 65535, 4200000000 – 4294967294) from the `AS_PATH` list of outbound prefixes of BGP neighbors that use this profile.

This option has no function for iBGP connections.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Replace

Replaces all private AS numbers in the `AS_PATH` with the AS number of the device.

Remove

Removes all private AS numbers from the `AS_PATH`.

No

Leaves all of the private AS numbers in the `AS_PATH`.

Default:

No

2.93.1.3.8 AS override

Enables or disables the overriding of AS numbers in the `AS_PATH` outbound prefixes.

With this option enabled, the device replaces all of the AS numbers of the BGP neighbors with its own AS number.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Yes

Replaces all AS numbers of BGP neighbors in the `AS_PATH` with its own AS number.

No

Leaves all AS numbers of BGP neighbors in the `AS_PATH`.

Default:

No

2.93.1.3.10 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.3.11 Send-Default-Route

This switch determines the behavior of the propagation of default routes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Yes

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table (*2.93.1.6.1 IPv4* on page 1724 or *2.93.1.6.2 IPv6* on page 1726).

Default:

No

2.93.1.3.12 Connect-Retry-Time

Specifies the time in seconds that the router waits until the next connection attempt following a failed BGP connection attempt. Generally speaking, this option is only necessary to speed things up when the remote site is in the "passive" connection mode.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

120

2.93.1.4 Address family

Use this directory to configure the settings of the IPv4 and IPv6 parameters that apply to all of the devices of a BGP neighbor profile.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.4.1 IPv4

Use this table to configure the IPv4 settings that apply to all of the devices of a BGP neighbor profile.

By default, an "activated" entry named "DEFAULT" is already provided.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily**

2.93.1.4.1.1 Neighbor profile

Contains the name of the corresponding neighbor profile as saved under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.4.1.2 Rtg-Tag

This determines that the device only advertises the IPv4 routes set under **Setup** > **Routing-Protocols** > **BGP** > **Networks** > **IPv4** to the BGP neighbors if their routing tag matches the one configured here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.93.1.4.1.3 Operating

Enables or disables the distribution of IPv4 NLRI of this address family to the BGP neighbors that use this neighbor profile.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Yes

This entry is enabled. The device sends IPv4 routes to the BGP neighbors.

No

This entry is disabled. The device does not send IPv4 routes to the BGP neighbors, but depending on the setting it may send IPv6 routes.

Default:

No

2.93.1.4.1.4 Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options “Standard” and “Extended” are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Default

When activated, the device permits the standard community attributes in the NLRI in accordance with *RFC 1997*.

Advanced

When activated, the device permits the extended community attributes in the NLRI in accordance with *RFC 4360*.

Default:

Default

Advanced

2.93.1.4.1.5 Nexthop-Self

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

No

Leaves the IP address of the next hop in the NLRI unchanged.

Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

Default:

No

2.93.1.4.1.6 Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:

0

2.93.1.4.1.7 Local-Pref

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Local preference" is a BGP standard attribute (`LOCAL_PREF`) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 5 characters from `[0-9]`

0 … 99999

Default:

100

2.93.1.4.1.8 Prefix limit

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The prefix limit is disabled.

2.93.1.4.1.9 Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

RIP

The device redistributes RIP routes from the routing table to the BGP neighbors.

OSPF

The device distributes OSPF routes from the routing table to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

2.93.1.4.1.10 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.93.1.4.1.11 Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.4.1.12 Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Allow
Reject

Default:

Allow

2.93.1.4.2 IPv6

Use this table to configure the IPv6 settings that apply to all of the devices of a BGP neighbor profile.

By default, one "deactivated" entry named "DEFAULT" is already provided.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily**

2.93.1.4.2.1 Neighbor profile

Contains the name of the corresponding neighbor profile as saved under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.4.2.2 Rtg-Tag

This determines that the device only advertises the IPv6 routes set under **Setup** > **Routing-Protocols** > **BGP** > **Networks** > **IPv6** to the BGP neighbors if their routing tag matches the one configured here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.93.1.4.2.3 Operating

Enables or disables the distribution of NLRI of this address family to the BGP neighbors that use this neighbor profile.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Yes

This entry is enabled. The device sends IPv6 routes to the BGP neighbors.

No

This entry is disabled. The device does not send IPv6 routes to the BGP neighbors, but depending on the setting it may send IPv4 routes.

Default:

No

2.93.1.4.2.4 Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options “Standard” and “Extended” are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Default

When activated, the device permits the standard community attributes in the NLRI in accordance with *RFC 1997*.

Advanced

When activated, the device permits the extended community attributes in the NLRI in accordance with *RFC 4360*.

Default:

Default

Advanced

2.93.1.4.2.5 Nexthop-Self

Enables or disables the replacement in the NLRI of the next-hop attribute by the device's own IP address.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

No

Leaves the IP address of the next hop in the NLRI unchanged.

Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

Default:

No

2.93.1.4.2.6 Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:

0

2.93.1.4.2.7 Local-Pref

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Local preference" is a BGP standard attribute (`LOCAL_PREF`) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 5 characters from `[0-9]`

0 … 99999

Default:

100

2.93.1.4.2.8 Prefix limit

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The prefix limit is disabled.

2.93.1.4.2.9 Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

2.93.1.4.2.10 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.93.1.4.2.11 Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.4.2.12 Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Allow
Reject

Default:

Allow

2.93.1.5 Policy

Use this directory to configure the filter settings for outbound and inbound NLRIs.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.5.1 Default

The device applies this default policy for a BGP neighbor if it is unclear whether it should accept its prefix or not. The cause for this may be:

- There is no policy configured for this BGP neighbor.
- The specified filter does not exist.
- None of the filters specified under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters** applies.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

Possible values:

Permit

The device accepts the prefix from the BGP neighbor.

Deny

The device rejects the prefix from the BGP neighbor.

2.93.1.5.2 Overrides

This directory contains the list of possible manipulations to NLRIs. The actions in the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions** apply the overrides configured here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

2.93.1.5.2.1 Basic

This table contains overrides that manipulate the basic attributes of NLRIs.

If an action applies a row of this table, all of the manipulations that this row implements are processed.

The specification of basic attributes is optional. If you want the action to change just one basic attribute, enter the desired value at the appropriate place and leave the remaining attributes in their default setting.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**

2.93.1.5.2.1.1 Name

Contains the name of this modification.

This entry is referenced by the actions configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.2.1.2 Set-Weight

If configured, this entry causes the device to modify the weighting of an NLRI to the value specified here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 5 characters from `[0–9]`

Default:

0

Special values:

0

The device retains the original value of the NLRI.

2.93.1.5.2.1.3 Set-Local-Pref.

If configured, this entry causes the device to modify the local preference value of an NLRI to the value specified here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 10 characters from `[0–9]`

Default:

0

Special values:

0

The device retains the original value of the NLRI.

2.93.1.5.2.1.4 Remove-MED

If configured, the device deletes the multi-exit discriminator (MED) of an NLRI before it processes the setting under **Set-MED**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

No

The MED remains in the NLRI.

Yes

The device deletes the MED of the NLRI.

Default:

No

2.93.1.5.2.1.5 Set-MED

If configured, this entry causes the device to modify the multi-exit discriminator (MED) of an NLRI to the value specified here. If the NLRI contains no MED, the device creates this attribute.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The device retains the original value of the NLRI.

2.93.1.5.2.1.6 Set-Nexthop

If configured, this entry causes the device to modify the next-hop IP address of an NLRI to the value specified here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Special values:

empty

The device retains the original value of the NLRI.

`self`

The device replaced the next-hop IP address with its own IP address.

2.93.1.5.2.1.7 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.93.1.5.2.1.8 Set-Link-Local-Nexthop

If configured, this entry causes the device to modify the next-hop link-local IPv6 address of an NLRI to the value specified here. This only effects IPv6 prefixes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 39 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.93.1.5.2.1.9 Set-Admin-Distance

This parameter specifies the “administrative distance” given to prefixes received in the BGP when they are entered into the routing table. The list of fixed “administrative distances” for the various system services and routing protocols can be displayed on the CLI by show admin-distance.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 3 characters from `[0-9]`

2.93.1.5.2.2 AS-Path

This table contains overrides that manipulate the `AS_PATH` attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Filter private**
2. **Replace**
3. Together **Prepend count** and **Prepend**

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**

2.93.1.5.2.2.1 Name

Contains the name of this modification.

This entry is referenced by the actions configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.2.2.2 Filter private AS

If configured, this entry causes the device to modify the specification of the private AS numbers in the `AS_PATH` attribute of an NLRI in accordance with this setting.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Replace

The device replaces the existing private AS numbers with the AS number of the current BGP instance.

Remove

The device removes all private AS numbers.

No

The device retains the existing private AS numbers of the NLRI.

Default:

No

2.93.1.5.2.2.3 Replace

If configured, this entry causes the device to change the `AS_PATH` attribute of the NLRI to the value specified here.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Max. 62 characters from `[0-1],`

Default:

empty

Special values:

empty

The device retains the original value of the NLRI.

2.93.1.5.2.2.4 Prepend

If configured, this entry causes the device to prepend the `AS_PATH` attribute of the NLRI with the value entered here as often as is specified under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path** > **Prepend-Count**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Special values:

empty

The device retains the original value of the NLRI.

self

The device prepends the `AS_PATH` attribute of the NLRI with its own AS number.

last

The device prepends the `AS_PATH` attribute of the NLRI with the most recently used AS number.

2.93.1.5.2.2.5 Prepend count

Determines how often the device prepends the `AS_PATH` attribute of the NLRI with an AS number.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

Special values:

0

The device retains the original value of the NLRI even if an entry is configured under **Prepend**.

2.93.1.5.2.2.6 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.2.3 Communities

This table contains overrides that manipulate the Communities attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Delete**
2. **Add**
3. **Remove**

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**

2.93.1.5.2.3.1 Name

Contains the name of this modification.

This entry is referenced by the actions configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.2.3.2 Clear

Determines whether the device deletes unknown communities from the NLRI.

Known communities remain in place even if this option to set to “Yes”.

Known communities are:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

For more information, please see *RFC 1997* and *RFC 3765*.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**

Possible values:

Yes

The device deletes unknown communities from the NLRI.

No

The device does not change the communities of an NLRI.

Default:

No

2.93.1.5.2.3.3 Add alarm

Specifies which communities the device adds to an NLRI.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**

Possible values:

Max. 62 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.93.1.5.2.3.4 Remove

Specifies which communities the device removes from an NLRI.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

Known communities are not removed from NLRI. Known communities are:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

The following input formats are available for communities:

Input format	Community
1:2	Standard community
1.2.3.4:1	IPv4-specific extended community
roc:1.2.3.4:1	IPv4-specific route origin extended community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4-specific route target extended community
ext2:1:2	Two-byte AS extended community
ext4:1:2	Four-byte AS extended community
roc:1:2	Two-byte AS route origin extended community (Site-of-Origin (SoO))
rtc:1:2	Two-byte AS route origin extended community
roc:ext4:1:2	Four-byte AS route origin extended community (Site-of-Origin (SoO))

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**

Possible values:

Max. 62 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.2.3.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.2.4 Large-Communities

This table contains overrides that manipulate the large community attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Clear**
2. **Add**
3. **Remove**

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**

2.93.1.5.2.4.1 Name

Contains the name of this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.2.4.2 Clear

Determines whether the device deletes unknown large communities from the NLRI.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Yes

The device deletes unknown large communities from the NLRI.

No

The device does not change the large communities of an NLRI.

Default:

No

2.93.1.5.2.3.3 Add alarm

Specifies which large communities the device adds to an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global Administrator or ASN>:<Local Data Part 1>:<Local Data Part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

2.93.1.5.2.4.4 Remove

Specifies which large communities the device removes from an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global Administrator or ASN>:<Local Data Part 1>:<Local Data Part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

2.93.1.5.2.4.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.3 Actions

This table lists actions that carry out modifications to NLRIs.

The modifications carried out by each action are specified in the directory **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

2.93.1.5.3.1 Name

Contains the name of this action.

This entry is referenced by the actions entered under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.3.2 Basic

Contains the name of an override of basic entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.3.3 AS-Path

Contains the name of an override of `AS_PATH` entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.3.4 Community

Contains the name of an override of Community entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.3.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.3.6 Large-Communities

Contains the name of an override of large-community entries in the NLRI.

This entry refers to the entries in the override table under *2.93.1.5.2.4 Large-Communities* on page 1709.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

2.93.1.5.4 Lists

This directory contains definitions used by BGP filters to identify NLRIs and execute the corresponding actions.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

2.93.1.5.4.1 Prefix

This table contains prefix lists that are used to identify NLRIs based on their network (prefix) and netmask (prefix length).

An entry can contain several prefixes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists**

2.93.1.5.4.1.1 Name

Contains the name of this prefix list.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.4.1.2 IP address

Contains the IPv4 or IPv6 address of the network.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.93.1.5.4.1.3 Prefix-Length

Contains the netmask or prefix length of the network.

This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address.

The prefix length of the NLRI must exactly match this value unless **Length-min** and **Length-max** are set to values not equal to zero.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

The network of the NLRI matches if it comes from same IP address family as that specified under **IP address**.

2.93.1.5.4.1.4 Length-Min

Specifies the minimum prefix length value that the network of the NLRI needs in order to match.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

2.93.1.5.4.1.5 Length-Max

Specifies the maximum prefix length value that the network of the NLRI needs in order to match.

If this entry is less than the value for **Prefix-Min**, the value "0" applies.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

No maximum prefix length.

2.93.1.5.4.1.6 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefix**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.4.2 AS-Path

This table contains AS-path lists in order to identify NLRIs by their `AS_PATH` attributes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists**

2.93.1.5.4.2.1 Name

Contains the name of this AS-path list.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Path**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.4.2.2 AS Path Regex

Contains a regular expression that checks the `AS_PATH` of the NLRI. Examples:

- `.*_100`: filters all NLRIs originating from “AS100”.
- `.*_(100|200)`: filters all NLRIs originating from “AS100” or “AS200”.
- `100_(.*_)?(500|400)_.*`: filters all NLRIs from the BGP neighbor with the AS number “AS100”, which were also previously routed via networks with the AS numbers “AS500” or “AS400” (or both).
- `100_(500|400|123)_.*`: filters all NLRIs from the BGP neighbor with the AS number “AS100” and which received this number beforehand directly from BGP neighbors with the AS numbers “AS500”, “AS400” or “AS123”.
- `100_(100_)*(300_)*300`: filters all NLRIs from the BGP neighbor with the AS number “AS100” and which received this number beforehand from the BGP neighbor with the AS number “AS300”. The expression also allows for AS prepend paths.

› `100_ 200`: filters all NLRIs from the BGP neighbor with the AS number “AS100” and which originated from the network with the AS number “AS200”. The route taken by the NLRIs from “AS200” to “AS100” is unimportant.

Expressions must be constructed in PERL syntax.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Path**

Possible values:

Max. 62 characters from `[0-9]$()*+-.?[\]^_{|}`

Default:

empty

Special values:

empty

This list entry applies to all `AS_PATH` attributes of the NLRI.

2.93.1.5.4.2.3 Regex-Match

Determines how closely the regular expression under **AS-Path-Regex** needs to match the `AS_PATH` attribute of the NLRI in order for the list entry to apply.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Path**

Possible values:

Full

The regular expression fully describes the `AS_PATH` attribute of the NLRI.

Partial

The regular expression only describes parts of the `AS_PATH` attribute.

Default:

Full

2.93.1.5.4.2.4 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Path**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.4.3 Communities

This table contains community lists in order to identify NLRIs by their community attributes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists**

2.93.1.5.4.3.1 Name

Contains the name of this community list.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Communities**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.4.3.2 Communities

Contains communities that the community attribute of the NLRI must match with.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Communities**

Possible values:

Max. 62 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.1.5.4.3.3 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.4.4 Large-Communities

This table contains large-community lists in order to identify NLRIs by their community attributes.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists**

2.93.1.5.4.4.1 Name

Contains the name of this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.4.4.2 Large-Communities

Contains large communities that the large-community attribute of the NLRI must match with.

The communities are specified in a comma-separated list.

Structure of a large community: *<Global Administrator or ASN>*`:`*<Local Data Part 1>*`:`*<Local Data Part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

2.93.1.5.4.4.3 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.5 Matches

This table combines list entries from the directory **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** to find matches between multiple list entries and NLRI.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

2.93.1.5.5.1 Name

Contains the name of this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.5.2 Prefix

Contains the corresponding entry from a prefix list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefixes**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Special values:

empty

Handles the NLRI as if there were a match with the prefix list.

2.93.1.5.5.3 AS-Path

Contains the corresponding entry from an AS-path list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Paths**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 80 characters from `[A-Z][a-z][0-9]-_,`

Default:

empty

Special values:

empty

Handles the NLRI as if there were a match with the AS-path list.

2.93.1.5.5.4 Communities

Contains the corresponding entry from a communities list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Communities**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 80 characters from `[A-Z][a-z][0-9]-_,`

Default:

empty

Special values:

empty

Handles the NLRI as if there were a match with the communities list.

2.93.1.5.5.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.5.5.6 Large-Communities

Contains the corresponding item in the list under *2.93.1.5.4.4 Large-Communities* on page 1718.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 80 characters from `[A-z][a-z][0-9],-_`

Default:

empty

2.93.1.5.5.7 RPKI-State

The Resource Public Key Infrastructure (RPKI) status of prefixes can be used in a BGP policy, so rules can apply it to a BGP prefix. The rejection of invalid prefixes is not recommended; instead, they should be given a lower preference. In this case, a BGP rule is defined that matches to the RPKI status “Invalid”. The action sets the preference of this prefix to the value 10, for example. Once a prefix has been rejected, it is not saved and is no longer available unless the prefix is retransmitted and reevaluated by the BGP neighbor.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

None

The RPKI state is not processed.

Not-found

The entry matches if the PRKI state of the prefix is set to “Not-found”.

Valid

The entry matches if the PRKI state of the prefix is set to “Valid”.

Invalid

The entry matches if the PRKI state of the prefix is set to “Invalid”.

2.93.1.5.6 Filters

This table contains filters that an NLRI to or from a BGP neighbor must pass through if the neighbor is configured with a corresponding policy.

For multiple filter entries with the same name, the device processes the filters according to the configured priority, until a filter matches the NLRI. The device then stops the filter pass.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy**

2.93.1.5.6.1 Name

Contains the name of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.6.2 Priority

Sets the priority of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value. A higher value means a higher priority.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.93.1.5.6.3 Address family

Specifies the address family for which this filter applies.

If no option is selected, the entry is disabled.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

IPv4
IPv6

Default:

IPv4

IPv6

2.93.1.5.6.4 Matches

Specifies the name of an entry from the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Match**.

The device applies this filter if the NLRI matches the criteria.

If this field indicates an invalid name, the device denies the NLRI and performs no further filters in the current filter chain.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Max. 80 characters from `[0-9][A-Z][a-z]-_,!`

Default:

empty

Special values:

empty

The device treats the NLRI as if it did match the criteria.

2.93.1.5.6.5 Policy

Specifies whether the device should further process the filtered NLRI in the case that the filter is valid for the NLRI.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Deny

No further processing.

Permit

The device processes the NLRI further.

Default:

Deny

2.93.1.5.6.6 Action

Specifies which of the actions from the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions** is applied by the device to the NLRI.

If this field is empty or refers to an invalid name, the device performs no action.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.1.5.6.7 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Filters**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.93.1.6 Networks

Use this directory to configure the networks that the device shares with the BGP neighbors.

The distribution of these networks depends on the setting under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4/IPv6** > **Operating**.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.6.1 IPv4

Use this directory to configure the IPv4 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**.

The minimum specification for a valid new entry is one **IP address**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks**

2.93.1.6.1.1 IP address

Contains the IPv4 address or the prefix of the network.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

2.93.1.6.1.2 Netmask

Includes the IPv4 netmask of the network.

The route is the default route for this address family if this entry contains the default setting `0.0.0.0`.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

2.93.1.6.1.3 Rtg-Tag

Contains the routing tag for this network.

The table under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4** uses this entry to filter the communication with BGP neighbors.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv4**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.93.1.6.1.4 Type

This item specifies whether the device advertises this network always or only when it appears in the active routing table.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv4**

Possible values:

Static

The network is always selected for advertisement.

Dynamic

The network is only selected for advertisement when it appears in the active routing table.

Default:

Static

2.93.1.6.1.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv4**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.93.1.6.2 IPv6

Use this directory to configure the IPv6 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**.

The minimum specification for a valid new entry is one **prefix**.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks**

2.93.1.6.2.1 Prefix

Contains the prefix (IPv6 address portion) of the network.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv6**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.93.1.6.2.2 Prefix-Length

Contains the prefix length of the IPv6 network.

The route is the default route for this address family if this entry contains the default setting `0`.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv6**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

2.93.1.6.2.3 Rtg-Tag

Contains the routing tag for this network.

The table under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6** uses this entry to filter the communication with BGP neighbors.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv6**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.93.1.6.2.4 Type

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv6**

Possible values:

Static
The device always uses this network in advertisements.

Dynamic
The device only uses this network in advertisements when it appears in the active routing table.

Default:

Static

2.93.1.6.2.5 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **BGP** > **Networks** > **IPv6**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.93.1.7 Operating

Enables or disables BGP in the device.

With BGP disabled, the BGP-related `show` console commands have no function.

Console path:

Setup > **Routing-Protocols** > **BGP**

Possible values:

Yes
BGP is enabled in the device.

No
BGP is disabled in the device.

Default:

No

2.93.1.8 Auto-Restart

Specifies whether a BGP neighbor automatically restarts after an error.

Console path:

Setup > **Routing-Protocols** > **BGP**

Possible values:

Yes

The automatic restart is enabled.

No

The automatic restart is disabled.

Default:

Yes

2.93.1.9 Manual-Start

This action is used to start a BGP neighbor that was previously stopped by means of a manual stop.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from `[A-Z][a-z][0-9]-_`).

If the arguments entered here match for several neighbors, the device establishes a connection to each one of them.

The specified neighbors need to meet the following requirements:

- They must be fully configured for BGP.
- For each one, the **Connection mode** setting under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** must not be set to "passive".

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.10 Manual stop

With this action, you manually stop a BGP neighbor.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from `[A-Z][a-z][0-9]-_`).

If the arguments entered here match for several neighbors, the device terminates all of these connections.

If multiple connections are opened to a neighbor, the device terminates all of these connections.

Optionally, a reason can be posted to the other BGP router as a message according to *RFC 8203*. Enter this reason as an additional parameter.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.11 Active start

Manually starts a BGP neighbor.

This function and its operating conditions are identical to **Manual start**, although in this case the device also connects to neighbors, for which the **Connection mode** under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** is set to "Passive".

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.12 Reboot

With this action, you manually restart a BGP neighbor.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from `[A-Z][a-z][0-9]-_`).

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.1.13 Global-Read-Only-Timer

Time in seconds that the device remains in read-only mode after being started. As long as the device is in read-only mode, it receives routes from BGP neighbors but does not perform the "shortest-path algorithm" for route computation. This means that it does not send routes to BGP neighbors. This switch is used to optimize the performance of central-site devices where many routes are possible. This means that the device only performs a route computation once it has received all of the possible routes.

Console path:

Setup > **Routing-Protocols** > **BGP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

The timer is deactivated.

2.93.1.14 Peer-Read-Only-Timer

Time in seconds per individual neighbor that the device remains in read-only mode after being started. As long as the device is in read-only mode, it receives routes from this BGP neighbor but does not perform the "shortest-path algorithm" for route computation. This means that it does not send routes to this BGP neighbor. As soon as a BGP neighbor has sent its routes and issues an `End-Of-RIB` marker, the receiving device automatically exits the read-only mode and

starts route computation. LANCOMRouters automatically send an `End-Of-RIB` marker after successfully transmitting its routes to a neighbor.

Console path:

Setup > **Routing-Protocols** > **BGP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

The timer is deactivated.

2.93.1.15 Send-Refresh-Request

This action sends a `BGP-Route-Refresh` message to a BGP neighbor. If this neighbor supports the `Route-Refresh` option, it sends its routes once again. The `Route-Refresh` option allows routes to be received from a neighbor again without having to restart the BGP connection.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from `[A-Z][a-z][0-9]-_`). Optionally specify the address family IPv4 or IPv6.

Console path:

Setup > **Routing-Protocols** > **BGP**

2.93.2 Route monitor

In this directory, you configure the route monitor.

Console path:

Setup > **Routing-protocols**

2.93.2.1 Monitor table

In this table, you configure the route monitor.

Console path:

Setup > **Routing-protocols** > **Route-monitor**

2.93.2.1.1 Backup peer

Contains the name of the backup remote station.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.2.1.2 Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

2.93.2.1.3 Rtg-Tag

Contains the routing tag of the prefix being monitored.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.93.2.1.4 Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 10 characters from `[0-9]`

Default:

20

2.93.2.1.5 Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

No delay: The device immediately closes the connection to the backup peer when the prefix arrives.

2.93.2.1.6 Operating

Specifies whether this backup connection is enabled.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Yes

The backup connection is enabled.

No

The backup connection is disabled.

Default:

No

2.93.2.1.7 Comment

Comment on this entry.

Console path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.2.2 Operating

This action is used to enable or disable the route monitor.

Console path:

Setup > **Routing-protocols** > **Route-monitor**

Possible values:

No

The route monitor is disabled.

Yes

The route monitor is enabled.

Default:

No

2.93.3 OSPF

This directory enables you to configure the device for the Open Shortest Path First protocol.

Console path:

Setup > **Routing-Protocols**

2.93.3.1 OSPF instance

This table is used to configure the OSPF instances.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.1.1 OSPF instance

This parameter contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

2.93.3.1.2 Operating

Activates or deactivates this OSPF instance

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

No
Disabled

Yes
Enabled

Default:

Yes

2.93.3.1.3 Router ID

The 32-bit router ID of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.1.5 Rtg-Tag

Contains the routing tag assigned to this instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 65535

Default:

0

2.93.3.1.6 Advertise-Default-Route

Specifies whether this router should advertise or propagate the default route in this instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

No

The router does not advertise a default route.

Yes

The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

Default:

No

2.93.3.1.7 Intra-Area-Distance

Defines the administrative distance with which OSPF inserts incoming intra-area routes into the routing table.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 255

Default:

110

2.93.3.1.8 Inter-Area-Distance

Defines the administrative distance with which OSPF inserts incoming inter-area routes into the routing table.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 255

Default:

110

2.93.3.1.9 External-Distance

Defines the administrative distance with which OSPF inserts incoming external routes into the routing table.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 255

Default:

110

2.93.3.2 Areas

This table is used to configure the OSPF areas.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.2.1 OSPF instance

This parameter contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

2.93.3.2.2 Area ID

The area ID (displayed as an IPv4 address) identifies the area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

IPv4 address `[0-9.]`

Special values:

0.0.0.0

Designates this instance as the backbone area.

2.93.3.2.3 Type

This parameter describes the type of the area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

Normal
Stub

Default:

Normal

2.93.3.2.4 Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

0 … 4294967295

2.93.3.3 Area-Address-Aggregation

This table is used to configure the area address aggregation.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.3.1 OSPF instance

This parameter contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.3.2 Area ID

Contains the ID of the area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.3.3 IP address

This parameter contains the IPv4 address.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.3.4 IP netmask

This parameter contains the IPv4 subnet mask.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 netmask `[0-9.]`

2.93.3.3.5 Advertise

Enables or disables the advertisement of this address aggregation.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

No

Advertising disabled

Yes

Advertising enabled

Default:

No

2.93.3.4 Interfaces

Specifies the interfaces on which OSPF is operated.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.4.1 Interface

Contains the interface (IPv4 network or WAN remote site) on which OSPF is to be activated.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.4.2 OSPF-Instance

This parameter contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.4.3 Area-ID

Contains the ID of the area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.4.4 Type

Contains the interface type.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Broadcast

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

NBMA

Non-Broadcast Multi-Access. Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication. All neighbors must be configured manually.

2.93.3.4.5 Output-Ccost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

1 … 65535

2.93.3.4.6 Rxmt-Interval

Contains the number of seconds between retransmissions.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

2.93.3.4.7 Inf-Trans-Delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

2.93.3.4.8 Router-Priority

The priority of this router on this interface when it is set as default router (DR). The router with the highest priority is set as the default router.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 255

Special values:

0

The value 0 prevents the router from becoming default router on this interface.

2.93.3.4.9 Hello-Interval

The interval in seconds in which the router sends Hello packets from this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

2.93.3.4.10 Router-Dead-Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

2.93.3.4.11 Authentication-Type

Authentication method used for this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Null
Simple-Password
Cryptographic-MD5

Default:

Null

2.93.3.4.12 Authentication-Key

Authentication key for this network in the case that the authentication type **Null** is used.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

16 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

2.93.3.4.13 Passive

Defines whether OSPF works actively or passively on this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

No
Yes

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

Default:

No

2.93.3.4.14 MTU-Ignore

Disables the MTU value check in database description packets. This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

No
Yes

Default:

No

2.93.3.5 Virtual-Links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.5.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.5.2 Transit area ID

Defines the area ID of the transit area.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.5.3 Router ID

Defines the router ID of the router at the remote end of the virtual link.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.5.4 Authentication type

Authentication method used for this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

Null
Simple password
Cryptographic MD5

Default:

Null

2.93.3.5.5 Authentication key

Authentication key for this network in the case that the authentication type **Null** is used.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

16 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

2.93.3.5.6 Rxmt-Interval

Contains the number of seconds between retransmissions.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

2.93.3.5.7 Hello-Interval

The interval in seconds in which the router sends Hello packets from this interface.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

2.93.3.5.8 Router-Dead-Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

2.93.3.6 NBMA neighbors

The neighbors of your non-broadcast multi-access network are configured in the **NBMA neighbors** menu.

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.6.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.6.2 Interface

Contains the interface (IPv4 network or WAN remote site) on which OSPF is to be activated.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.6.3 IP address

Contains the IPv4 address of the neighbor router at the remote end.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.6.4 Poll-Interval

Defines the interval in which Hello messages are sent to this router.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

0 … 4294967295

Special values:

0

Disables the transmission of Hello messages.

2.93.3.6.5 Eligible-As-Designated-Router

Specifies whether the local device itself is selectable as default router.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

No
Yes

Default:

No

2.93.3.7 Point-to-multipoint neighbors

This table is used to configure your point-to-multipoint neighbors.

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network.

If no default router is selected, multicast is used for communications instead.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.7.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.7.2 Interface

Contains the interface (IPv4 network or WAN remote site) on which OSPF is to be activated.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.7.3 IP address

Contains the IPv4 address of the neighbor router at the remote end.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

2.93.3.7.4 Poll-Interval

Defines the interval in which Hello messages are sent to this router.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

0 … 4294967295

Special values:

0

Disables the transmission of Hello messages.

2.93.3.8 Operating

Enables or disables the Open Shortest Path First (OSPF) feature in the device.

Console path:

Setup > **Routing-Protocols** > **OSPF**

Possible values:

Yes

OSPF is enabled in the device.

No

OSPF is disabled in the device.

Default:

No

2.93.3.9 Route-Redistribution

In the **Route-Redistribution** menu you configure the redistribution of routes that were learned dynamically.

Console path:

Setup > **Routing-Protocols** > **OSPF**

2.93.3.9.1 BGP

in the **BGP** menu you configure the redistribution of routes that were learned dynamically from the Border Gateway Protocol.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution**

2.93.3.9.1.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.9.1.2 BGP instance

Contains the name of the BGP instance.

Console path:

Routing-Protocols > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.9.1.3 Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.3.9.1.4 Metric source

Specifies which source is used to set the OSPF metric.

Console path:

Routing-Protocols > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses the "local preference" value of the BGP prefix.

Default:

Constant

2.93.3.9.1.5 Constant-Metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

Console path:

Routing-Protocols > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

0 … 4294967295

2.93.3.9.1.6 Path type

Specifies the type of routes that were imported into OSPF.

Console path:

Routing-Protocols > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

External-Type-1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External-Type-2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

2.93.3.9.1.7 External-Route-Tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

Console path:

Routing-Protocols > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

0 … 4294967295

2.93.3.9.1.8 Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **BGP**

Possible values:

Accept
Deny

Default:

Accept

2.93.3.9.2 Connected

In the **Connected** menu you configure the redistribution of routes which are automatically entered into the routing table by the operating system.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution**

2.93.3.9.2.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.9.2.2 Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.3.9.2.3 Metric source

Specifies which source is used to set the OSPF metric.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

2.93.3.9.2.4 Constant-Metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

0 … 4294967295

2.93.3.9.2.5 Path type

Specifies the type of routes that were imported into OSPF.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

External-Type-1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External-Type-2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

2.93.3.9.2.6 External-Route-Tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

0 … 4294967295

2.93.3.9.2.7 Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Connected**

Possible values:

Accept
Deny

Default:

Accept

2.93.3.9.4 Static

In the **Static** menu you configure the redistribution of routes that are manually entered into the routing table by the user.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution**

2.93.3.9.4.1 OSPF instance

Contains the name of the OSPF instance.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.3.9.4.2 Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.3.9.4.3 Metric source

Specifies which source is used to set the OSPF metric.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

2.93.3.9.4.4 Constant-Metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

0 … 4294967295

2.93.3.9.4.5 Path type

Specifies the type of routes that were imported into OSPF.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

External-Type-1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External-Type-2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

2.93.3.9.4.6 External-Route-Tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

0 … 4294967295

2.93.3.9.4.7 Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Route-Redistribution** > **Static**

Possible values:

Accept
Deny

Default:

Accept

2.93.4 LISP

Settings for Locator / ID Separation Protocol (LISP).

Console path:

Setup > **Routing-Protocols**

2.93.4.1 Instances

This table contains the global configuration of the LISP instances on the device.

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.1.1 Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.1.2 Operating

Activates or deactivates this LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

No
Yes

2.93.4.1.3 EID-Rtg-Tag

Routing tag of the endpoint identifier (EID) of this instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.1.4 RLOC-Rtg-Tag

Routing tag of the routing locator (RLOC) of this instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.1.5 Instance-ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.1.6 Probing-Method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Off

The availability of the RLOCs is not checked periodically.

RLOC-Probing

The availability of the RLOCs is periodically checked by LISP RLOC messages.

2.93.4.1.8 IPv6

Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.4.1.9 Admin-Distance

Administrative routing distance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 3 characters from `[0-9]`

Default:

240

2.93.4.1.9 Accept-Unknown-ITRs

Defines whether the router should accept LISP data packets from unknown ITRs for which there is no map cache entry. This functionality is required especially for scenarios where PITR and PETR are operated via different servers or IP addresses.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Yes
No

Default:

No

2.93.4.2 EID-Mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.2.1 Name

References the name of the LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.2.2 EID-Address-Type

This bitmask specifies the protocol version of the EID prefix when referencing the EID prefix via an interface or network name.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

2.93.4.2.3 EID-Prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 43 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.2.4 Locator-Address-Type

This bitmask specifies the protocol version of the RLOC when referencing the EID prefix via an interface name.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

2.93.4.2.5 Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.2.6 Operating

Activates or deactivates this entry.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

No
Yes

2.93.4.2.7 Priority

The priority of the EID mapping.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

2.93.4.2.8 Weight

The weight of the EID mapping.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

2.93.4.2.9 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 25 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.3 ITR-Settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.3.1 Name

References the name of the LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.3.2 Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.93.4.3.3 Operating

Activates or deactivates these ITR settings.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

No
Yes

2.93.4.3.4 Loopback address

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.3.5 Rtg-Tag

Routing tag used to access the map resolver.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.3.6 Map-Resolver-Retries

Number of retries for map requests to the map resolver.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 3 characters from `[0-9]`

Default:

3

2.93.4.3.7 Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 18 characters from `[A-F][a-f][0-9]:.`

2.93.4.3.8 Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

2.93.4.4 ETR-Settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.4.1 Name

References the name of the LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.4.2 Map-Server

IPv4 or IPv6 address of the LISP map server

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.93.4.4.3 Operating

Activates or deactivates these ETR settings.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

2.93.4.4.4 Loopback address

Contains the sender address as the named interface that is used with the map server in LISP communication.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.4.5 Rtg-Tag

Routing tag to be used to access the map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.4.6 Map-Cache-TTL-Minutes

Time-to-live of the EID mappings in minutes registered with the map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.4.7 Map-Register-Interval-Seconds

Registration interval in seconds in which map registrations are sent to the map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

2.93.4.4.8 Key-Type

Algorithm used for authentication at the map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

None
HMAC-SHA-1-96
HMAC-SHA-256-128

2.93.4.4.9 Key

Key or password used to register the EID mapping on the map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.93.4.4.10 Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

2.93.4.4.11 Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

Console path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.93.4.5 Operating

This item switches the routing protocol Locator / ID Separation Protocol (LISP) on or off.

Console path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

2.93.4.7 Disable-TTL-Propagation

With this switch enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

Console path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

2.93.4.8 Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

Console path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

2.93.4.9 Native-Forward

If LISP networks are to communicate with non-LISP networks, proxy routers can be used. These roles are called Proxy Ingress Tunnel Router (Proxy-ITR) and Proxy Egress Tunnel Router (Proxy-ETR). If a LISP router receives a negative response from the map resolver, i.e. there is no mapping between requested EID to a RLOC, the LISP router can either send the

corresponding packets to a proxy xTR (Packet with LISP header) or via another local interface (package without LISP header).

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.9.1 Name

References the name of the LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.9.3 Type

Defines how packets should be sent to non-LISP networks.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

None
Packets to non-LISP networks are not forwarded and discarded.

ProxyXTR
Packets to non-LISP networks are sent to a proxy-xTR.

Interface
Packets to non-LISP networks are sent via a local interface.

2.93.4.9.4 Proxy-XTR

IPv4 or IPv6 address of the proxy XTR via which packets are sent to non-LISP networks.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

2.93.4.9.5 Interface

Name of the interface or remote site via which packets are sent to non-LISP networks.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.10 Redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.

Console path:

Setup > **Routing-Protocols** > **LISP**

2.93.4.10.1 Name

References the name of the LISP instance.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.10.2 Source

This bitmask specifies the route sources of the imported routes.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Connected

From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.

Static

The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

OSPF

The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

BGP

The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

2.93.4.10.3 Destination

Specifies the destination of routes imported to LISP.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Map-Cache

Imports the routes into the map cache. LISP performs map requests for these routes.

Eid-Table

Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

2.93.4.10.4 Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.93.4.10.5 Locator-Address-Type

Locator address type of the EID mapping used to import the imported prefixes into the EID table. Defines the protocol version of the RLOC when referencing the EID prefix using an interface name. Possible values:

IPv4

Only the IPv4 address is used as the RLOC of the referenced interface.

IPv6

Only the IPv6 address is used as the RLOC of the referenced interface.

IPv4+IPv6

Both the IPv4 address and the IPv6 address are used as RLOC of the referenced interface.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

IPv4
IPv6

2.93.4.10.6 Priority

Priority of the EID mapping with which the imported prefixes are imported into the EID table.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

2.93.4.10.7 Weight

Weight of the EID mapping used to import the imported prefixes into the EID table.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

2.93.4.10.8 Filter-List

Name of the prefix filter list from **Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**. Route redistribution is allowed for prefixes in this list.

Console path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.5 Filter

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP.

Console path:

Setup > **Routing-Protocols**

2.93.5.1 Prefix-List

Here you specify a prefix list that can be referenced by BGP.

Console path:

Setup > **Routing-Protocols** > **Filter**

2.93.5.1.1 Name

Contains the name of this entry. Prefixes that should belong to a list are referenced by the same name, e.g. List1.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.93.5.1.2 IP-Address

Contains the IPv4 or IPv6 address of the network.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

2.93.5.1.3 Prefix-Length

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Length-min** and **Length-max** are set to values not equal to zero.

If the value is “0”, the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.93.5.1.4 Length-Min

Specifies the minimum prefix length value required for the prefix to match.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.93.5.1.5 Length-Max

Specifies the maximum prefix length value required for the prefix to match.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

2.93.5.1.6 Comment

Comment on this entry.

Console path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.6 BFD

In this directory you configure the Bidirectional Forwarding Detection (BFD) protocol. BFD according to *RFC 5880* is a simple Hello protocol to detect the loss of a connection between two routers. Hello packets are sent by both routers at a set interval. If these Hello packets are not received within a certain interval, the connection is assumed to be broken. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

Adjusting the timer interval allows lost connections to be detected faster or slower. The lower the timer interval, the faster connection losses are detected.

- BFD supports IPv4 and IPv6.
- There is no echo mode.
- BFD is a protocol that requires significant system resources, CPU time and bandwidth. BFD is processed exclusively in software. Hardware processing is not supported for BFD.
- Setting the Hello to a very short interval may result in BFD flapping or the detection of false positives. If false positives occur, you should increase the Hello interval.
- We do not recommend setting the Hello interval at less than 250ms.

Console path:

Setup > **Routing-Protocols**

2.93.6.1 Key-Chains

This item is used to configure the key chains for BFD.

Console path:

Setup > **Routing-Protocols** > **BFD**

2.93.6.1.1 Name

Enter a descriptive name for this key chain. This name is used in the BFD profiles to reference this key chain.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Key-Chains**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

2.93.6.1.2 Number

Key chain number.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Key-Chains**

Possible values:

Max. 3 characters from `[0-9]`

2.93.6.1.3 Key

Key or password for this key chain.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Key-Chains**

Possible values:

Max. 80 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

2.93.6.2 Profiles

Configure the BFD profiles here.

Console path:

Setup > **Routing-Protocols** > **BFD**

2.93.6.2.1 Name

Enter a descriptive name for this BFD profile. If BFD is used in combination with BGP, this name is linked to the corresponding BGP neighbor.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

2.93.6.2.2 Min-Tx-Interval

Minimum interval in milliseconds between sent BFD control messages.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

1 … 9999

Default:

250

2.93.6.2.3 Min-Rx-Interval

Minimum interval in milliseconds between received BFD control messages.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

1 … 9999

Default:

250

2.93.6.2.4 Multiplier

Number of packets not received for an interface to be declared as down. The multiplier and the interval together produce the time until a connection is declared as down.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

1 … 255

Default:

3

2.93.6.2.6 Authentication

Specifies the type of authentication used for the BFD messages.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

None
Password
MD5
MD5-Meticulous
SHA1
SHA1-Meticulous

Default:

None

2.93.6.2.7 Key-Chain

Name of the key chain from the table *2.93.6.1 Key-Chains* on page 1775. Defines the key used for the BFD messages. For the parameter *2.93.6.2.6 Authentication* on page 1777, a value must be configured that is other than "None".

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

2.93.6.2.8 Mode

Specifies whether the BFD neighbor is single-hop or multi-hop connected. In single-hop mode, the UDP destination port 3784 and time-to-live of 1 are used in the IP header. Multi-hop mode uses UDP port 4784. In Automatic, single-hop mode is used if the route to the neighbor is of the type Connected LAN or WAN, otherwise multi-hop is used. By default, eBGP sessions are single-hop. iBGP sessions can be multi-hop.

Console path:

Setup > **Routing-Protocols** > **BFD** > **Profiles**

Possible values:

Automatic
Single-Hop
Multi-Hop

Default:

Automatic

2.93.6.3 Operating

Activates or deactivates BFD globally

Console path:

Setup > **Routing-Protocols** > **BFD**

Possible values:

No
Yes

Default:

No

2.93.7 RPKI

The Border Gateway Protocol (BGP) is susceptible to route hijacking, i.e. unauthorized routers can advertise routes and thus redirect data traffic from the actual destination to itself. This situation can be caused by erroneous configurations and by explicit attacks.

Resource Public Key Infrastructure (RPKI) is a cryptographic method for signing and validating routing data records, which consist of a prefix and an autonomous system (AS). This record is called the Route Origin Authorization (ROA). More information on RPKI can be found in *RFC 6480*.

LCOS supports the Resource Public Key Infrastructure to Router Protocol (RTR) as per *RFC 8210*, with which a validator or cache supplies the router with information about validated routes and the associated AS number. This information is used by the BGP process to check whether a prefix or route was sent from the correct origin AS. Also checked is whether the prefix length corresponds to the information from the ROA data set.

This cache either runs on its own server for its own prefixes, or a public validator is used.

Public RPKI caches contain a large number of ROA entries. The recommendation is to operate RPKI only on devices with sufficient main memory to meet requirements (i.e. more than 2 GB), meaning that central-site devices or the vRouter need a correspondingly large main memory.

This directory contains the configuration for the RPKI.

Console path:

Setup > **Routing-Protocols**

2.93.7.1 Caches

The RPKI validator or RPKI cache used are configured in this table. The supported transport protocol is TCP.

Console path:

Setup > **Routing-Protocols** > **RPKI**

2.93.7.1.1 Cache

IPv4, IPv6 address, or hostname where the RPKI cache is reached.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.93.7.1.2 Preference

Preferred cache where multiple caches are used. Lower values result in a higher preference.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

2.93.7.1.3 Loopback

You can optionally specify a source address that the RPKI client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

0

2.93.7.1.4 Rtg-Tag

Enter the routing tag for setting the route to the cache.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

0 … 65535

Default:

0

2.93.7.1.5 Port

The port of the RPKI cache.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 5 characters from `[0-9]`

Default:

323

2.93.7.1.6 Version

Protocol version of the PRKI-RTR protocol operated.

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Null

Protocol version 0 is used to communicate with the cache.

One

Protocol version 1 is used to communicate with the cache.

Fallback

Communication with the cache starts with version 1 and falls back to version 0 if necessary.

2.93.7.2 Operating

Activates or deactivates RPKI

Console path:

Setup > **Routing-Protocols** > **RPKI**

Possible values:

No
Yes

Default:

No

2.93.7.3 Accepted-Prefix-Type

Specifies which ROA prefix types (IPv4 or IPv6) should be stored. To optimize the main memory, the prefix type is recommended to be restricted to the address family (IPv4, IPv6) that is actually operated.

Console path:

Setup > **Routing-Protocols** > **RPKI**

Possible values:

Both

Both IPv4 and IPv6 RPKI records are stored on the device.

IPv4

Only IPv4 RPKI records are stored on the device.

IPv6

Only IPv6 RPKI records are stored on the device

Default:

Both

2.96 Iperf

iPerf measures the throughput for TCP and UDP applications, as well as latency, jitter, packet loss or packet reordering for UDP connections.

Use this menu to configure the iPerf settings.

Console path:

Setup

2.96.1 Server daemon

This menu contains the configuration for the iPerf server daemon.

Console path:

Setup > **Iperf**

2.96.1.1 Operating

This entry is used to enable or disable the iPerf server daemon.

Console path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

No

The iPerf server daemon is not active.

Yes

The iPerf server daemon is active.

Default:

No

2.96.1.2 Transport

Use this entry to set the transfer protocol used by the iPerf server daemon.

Console path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

UDP
TCP

Default:

UDP

2.96.1.3 Port

Here you specify a port on which the iPerf server expects packets to arrive.

Console path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

Max. 5 characters from `[0-9]`

Default:

5001

2.96.2 IPv4-WAN-Access

Here you determine whether measurements are also permitted over a WAN connection.

Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

Console path:

Setup > **Iperf**

Possible values:

No

Bandwidth measurements are not permitted over a WAN connection.

VPN

The bandwidth measurements are permitted over a WAN connection, but only if it is protected by a VPN tunnel.

Yes

Bandwidth measurements are also permitted over a WAN connection.

Default:

No

2.96.3 IPv4-Access-List

In order restrict iPerf access to certain stations only, enter the connection data into this table.

Console path:

Setup > **Iperf**

2.96.3.1 IP address

Enter the IPv4 address of the remote station.

Console path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

2.96.3.2 Netmask

Enter the netmask of the remote station.

Console path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

255,255,255,255

2.96.3.3 Rtg-Tag

Enter the routing tag that specifies the connection to the remote station.

Console path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.96.3.4 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.97 Battery Pack

This menu contains the configuration options of the Battery Pack.

Console path:

Setup

2.97.1 Operating

This entry shows whether the connected Battery Pack is operational.

Console path:

Setup > **Battery-Pack**

Possible values:

No
Yes

Default:

Yes

2.97.2 E-mail address

Enter the recipient of the status messages here.

Console path:

Setup > **Battery-Pack**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.97.3 Restart

Use this command to restart individual power outlets (Out 1 or Out 2). This interrupts the power supply to the device, so causing it to reboot.

Use the syntax `do restart 1`, for example.

Console path:

Setup > **Battery-Pack**

2.97.4 Alerting

Use this table to configure the messaging settings for the corresponding entries.

Console path:

Setup > **Battery-Pack**

2.97.4.1 Event

Name of the event for which the messaging settings are to be configured.

Console path:

Setup > **Battery-Pack** > **Alerting**

2.97.4.2 Mail

Enables or disables e-mail notifications for the selected event.

Console path:

Setup > **Battery-Pack** > **Alerting**

Possible values:

No
Yes

Default:

Yes

2.97.4.3 SNMP

Enables or disables SNMP notifications for the selected event.

Console path:

Setup > **Battery-Pack** > **Alerting**

Possible values:

No
Yes

Default:

Yes

2.97.4.4 Syslog

Enables or disables Syslog notifications for the selected event.

Console path:

Setup > **Battery-Pack** > **Alerting**

Possible values:

No
Yes

Default:

Yes

2.97.5 Discharge

This command is used to intentionally discharge the Battery Pack. Use the syntax `do discharge <start/stop>`.

If the command is executed with the parameter `start`, the Battery Pack starts to discharge. The parameter `stop` terminates the discharging of the Battery Pack.

Console path:

Setup > **Battery-Pack**

2.100 LBS

This is where you configure the settings for the LANCOM location-based services (LBS).

Console path:

Setup

2.100.1 Operating

Enables or disables the location-based services.

Console path:

Setup > **LBS**

Possible values:

Yes
No

Default:

No

2.100.2 Description

Enter a description of the device.

Console path:

Setup > **LBS**

Possible values:

Max. 251 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.100.3 Floor

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Console path:

Setup > **LBS**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

0

2.100.4 Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Console path:

Setup > **LBS**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

0

2.100.5 Coordinates

This table is used to set the coordinates of the device location. The position is defined in geographical coordinates (degrees, minutes, seconds, orientation).

Console path:

Setup > **LBS**

2.100.5.1 Index

This column specifies whether the entry defines the latitude or longitude.

You cannot change this entry.

Console path:

Setup > **LBS** > **Coordinates**

Possible values:

Latitude
Longitude

2.100.5.6 Decimal-Degree

Contains the decimal degrees of latitude.

Console path:

Setup > **LBS** > **Coordinates**

Possible values:

Max. 12 characters from `[0-9].`

Default:

empty

2.100.6 LBS-Server-Address

Enter the address of the LBS server.

Console path:

Setup > **LBS**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.100.7 LBS-Server-Port

Enter the port used by the LBS server.

Console path:

Setup > **LBS**

Possible values:

Max. 4 characters from `[0-9]`

Default:

9090

2.100.9 TLS-Client-Settings

In this menu, you configure the settings for a SSL/TLS secured connection to the LBS server.

Console path:

Setup > **LBS**

2.100.9.1 Versions

Here, select the encryption protocols for the SSL/TLS connection.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default:

SSLv3

TLSv1

2.100.9.2 Keyex-Algorithms

Here, select the encryption method for the SSL/TLS connection.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.100.9.3 Crypto-Algorithms

Here, select the crypto algorithms for the SSL/TLS connection.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.100.9.4 Hash-Algorithms

Here, select the hash algorithms for the SSL/TLS connection.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

MD5
SHA1
SHA-2-256
SHA2-384

Default:

MD5

SHA1

SHA-2-256

SHA2-384

2.100.9.5 Prefer-PFS

Specify whether PFS (perfect forward secrecy) is enabled for the SSL/TLS secured connection.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

Yes
No

Default:

Yes

2.100.9.7 Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

2.100.9.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **LBS** > **TLS-Client-Settings**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA

Default:

SHA1-RSA

SHA224-RSA

SHA256-RSA

SHA384-RSA

SHA512-RSA

2.100.10 Loopback-Address

Enter the LBS loopback address here.

Console path:

Setup > **LBS**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.100.11 Cache-Operating

Enable or disable the LBS cache here.

Console path:

Setup > **LBS**

Possible values:

No
Yes

2.100.12 Cache-Size

Enter the size of the LBS cache here.

Console path:

Setup > **LBS**

Possible values:

Max. 10 characters from `0123456789`

2.100.13 User-Name

Specify the user name for authorization at the LBS server.

Console path:

Setup > **LBS**

Possible values:

Max. 64 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.100.14 Password

Specify the password for authorization at the LBS server.

Console path:

Setup > **LBS**

Possible values:

Max. 64 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.100.15 Aggregation

Use this entry to determine whether larger amounts of data are to be aggregated.

Console path:

Setup > **LBS**

Possible values:

Yes
No

Default:

No

2.100.16 Measurements-Fields

This menu contains the settings for the LBS measurement fields.

Console path:

Setup > **LBS**

2.100.16.1 Sequence-Number-Transmit

This entry determines whether the sequence number is transmitted.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.2 SSID-Transmit

Determines whether the device transmits the SSID, which was sent by the WLAN client in its management frames, to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.3 Interface-Identifier-Transmit

This entry specifies whether the device sends the name of the interface used to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.4 BSSID-Transmit

Determines whether the device transmits the BSSID, which was sent by the WLAN client in its management frames, to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.5 Signal-Level-Transmit

Determines whether the signal strength observed for the WLAN client is transmitted to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.6 Frequency-Transmit

This entry determines whether the frequency used by the device is transmitted to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.7 Noise-Transmit

Determines whether the device transmits the noise level to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.16.8 WLAN-Frame-Type-Transmit

Determines whether the device transmits the WLAN-Frame-Type to the LBS server.

Console path:

Setup > **LBS** > **Measurements-Fields**

Possible values:

Yes
No

Default:

Yes

2.100.17 LBS-Server-Type

Here you configure whether the HTTP API uses JSON-format data packets or the Thrift API.

Console path:

Setup > **LBS**

Possible values:

Apache-Thrift
HTTP-JSON

2.100.18 HTTP-Server

This item determines the settings of the HTTP server when using the HTTP API.

Console path:

Setup > **LBS**

2.100.18.1 URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. If you use HTTPS, a PKCS#12 container with CA and client certificate must also be uploaded to the device. This can be done using LANconfig or WEBconfig.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.100.18.2 Loopback address

Use this item to configure which loopback address should be used for communication with the HTTP endpoint. This may be necessary if multiple IP networks are configured on the device.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.100.18.3 Secret

The HTTP server secret is transmitted in the JSON messages from the access point to the end point and can be used to additionally authenticate the messages.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.100.18.4 Data-Sources

Here you configure whether to transmit WLAN, BLE, or both types of LBS data.

The setting **BLE** is only supported on devices featuring BLE.

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

WLAN
BLE

2.101 Layer-7 app detection

This menu is used to configure layer-7 application detection.

Console path:

Setup

2.101.1 Operating

This entry is used to enable or disable layer-7 application detection.

Console path:

Setup > **Layer-7-App-Detection**

Possible values:

No
Yes

Default:

No

2.101.2 IP port applications

Set the target ports for the layer-7 application detection, or add new entries to the table.

Console path:

Setup > **Layer-7-App-Detection**

2.101.2.1 Application name

Specify a unique name for this application.

Console path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.101.2.2 Targets

Define targets for this application.

Specify multiple targets with a comma-separated list.

Console path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.101.2.3 Ports

Specify the ports to be tracked.

Console path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.101.4 Port table

Here you activate or deactivate the ports to be tracked by layer-7 application detection.

The contents of the table are device dependent.

Console path:

Setup > **Layer-7-App-Detection**

2.101.4.2 Port

This entry contains the name of the port selected from the table.

Console path:

Setup > **Layer-7-App-Detection** > **Port-Table**

2.101.4.3 Traffic tracking

This entry is used to enable or disable the tracking of traffic for this port.

Console path:

Setup > **Layer-7-App-Detection** > **Port-Table**

Possible values:

No
Yes

Default:

No

2.101.5 Status-Update-In-Minute

This entry sets an interval in minutes when the usage statistics are updated.

Console path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

2.101.6 Max queue length

This entry specifies the maximum queue length for the usage statistics.

Console path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

10000

2.101.7 Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

Console path:

Setup > **Layer-7-App-Detection**

2.101.11 VLAN

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

Console path:

Setup > **Layer-7-App-Detection**

2.101.11.1 VLAN-ID

Use this entry to specify a VLAN ID.

Console path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

0 … 65535

Default:

0

2.101.11.2 Track user

With this entry you enable or disable the tracking of user-specific data (user or client name and MAC address).

Console path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

2.101.11.3 Tracking active

This entry is used to enable or disable the tracking of general or application-specific data.

Console path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

2.101.12 Save-In-Min

Specify the interval in minutes for storing the usage statistics of the layer-7 application detection.

Console path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3600

2.102 LMC

In this menu, you configure the cloud parameters for the LMC (LANCOM Management Cloud).

Console path:

Setup

2.102.1 Operating

With this entry you enable or disable the ability to manage your LANCOM device with the LMC.

Console path:

Setup > **LMC**

Possible values:

No

The device does not connect to the LMC.

Yes

LMC is used to manage the device. If not done already, you need to conduct a first-time pairing of the device with the LANCOM Management Cloud. This is the default setting for devices without a WLAN interface.

Please note that without this pairing, it is not possible for the device to communicate with the Management Cloud.

Only without WLC

Devices within a network managed by a WLC do not connect to the LMC. This is the default setting for devices with a WLAN interface.

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:

Yes

2.102.12 Loopback address

Use this entry to set a loopback address for the LANCOM Management Cloud.

Console path:

Setup > **LMC**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

2.102.13 Configuration via DHCP

This entry enables or disables the reception of information via DHCP option 43, which is required to connect to the LMC.

Console path:

Setup > **LMC**

Possible values:

No
Yes

Default:

Yes

2.102.14 DHCP status

This menu contains the status values relating to the LMC domain that the device obtained via DHCP option 43.

Console path:

Setup > **LMC**

2.102.14.5 DHCP LMC domain

This entry shows the LMC domain obtained by the device via DHCP option 43.

Console path:

Setup > **LMC**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

cloud.lancom.de

2.102.15 LMC domain

Enter the domain name for the LANCOM Management Cloud here.

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]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

cloud.lancom.de

2.102.16 Rollout-Project-ID

Enter the project ID of this device in the LANCOM Management Cloud (LMC). It is assigned accordingly the first time it is connected to the LMC.

Console path:

Setup > **LMC**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.102.17 Rollout-Location-ID

Enter the location of this device in the LANCOM Management Cloud (LMC) here. It is assigned accordingly the first time it is connected to the LMC.

Console path:

Setup > **LMC**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.102.18 Rollout-Device-Role

Enter the role of this device in the LANCOM Management Cloud (LMC) here. It is assigned accordingly the first time it is connected to the LMC.

Console path:

Setup > **LMC**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.102.19 Management-Settings

This menu contains internal values that are managed by the LMC and that must not be changed.

Console path:

Setup > **LMC**

2.102.19.1 DynDNS

This menu contains internal values for the Dynamic DNS feature. They are managed by the LMC and must not be changed.

Console path:

Setup > **LMC** > **Management-Settings**

2.102.19.1.1 Peer

This is an internal value of the Dynamic DNS feature that is managed by the LMC and must not be changed.

Console path:

Setup > **LMC** > **Management-Settings** > **DynDns**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.19.1.2 Domain

This is an internal value of the Dynamic DNS feature that is managed by the LMC and must not be changed.

Console path:

Setup > **LMC** > **Management-Settings** > **DynDns**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.19.1.3 Source

This is an internal value of the Dynamic DNS feature that is managed by the LMC and must not be changed.

Console path:

Setup > **LMC** > **Management-Settings** > **DynDns**

Possible values:

Local

Report the locally configured IP to the LMC.

Remote

Report the remotely determined IP to the LMC.

2.103 Provisioning server

Use this menu to configure the provisioning server that handles the automated deployment of IT resources.

Console path:

Setup

2.103.1 Operating

This entry enables or disables the provisioning server.

Console path:

Setup > **Provisioning-Server**

Possible values:

No
Yes

Default:

Yes

2.103.2 Port

This entry specifies the port for the provisioning server.

Console path:

Setup > **Provisioning-Server**

Possible values:

0 … 65535

Default:

9999

2.103.3 Url

Specify the URL of the provisioning server.

Console path:

Setup > **Provisioning-Server**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.103.4 Url-via-DHCP

Here you enable or disable the device from obtaining the provisioning server URL via DHCP.

Console path:

Setup > **Provisioning-Server**

Possible values:

No
Yes

Default:

No

2.103.5 Secure port

Specify a secure port for the connection to the provisioning server here.

Console path:

Setup > **Provisioning-Server**

Possible values:

0 … 65535

Default:

1001

2.103.6 Polling-In-Minutes

This entry contains the time after which a device checks the provisioning server for any changes.

Console path:

Setup > **Provisioning-Server**

Possible values:

0 … 65535 Minutes

Default:

1140

2.103.7 Update server

With this entry, you specify the update server for the provisioning server.

Console path:

Setup > **Provisioning-Server**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104 Bonjour proxy

This menu contains the settings for the Bonjour proxy. The Bonjour proxy allows Bonjour services to be discovered across network boundaries.

Console path:

Setup

2.104.1 Operating

This entry is used to enable or disable the Bonjour proxy.

Console path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

No

2.104.2 Query client interval

Set the interval in minutes in which the query client requests the Bonjour services configured in the **Query client** table.

Console path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 999 Minutes

Default:

15

Special values:

0

2.104.3 Network list

Use this table to specify the networks between which Bonjour services may be discovered.

Console path:

Setup > **Bonjour-Proxy**

2.104.3.1 Name

Specify a unique name for this table entry.

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.104.3.2 Active

This entry is used to enable or disable the Bonjour proxy for the corresponding combination of client and server network.

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

No
Yes

Default:

No

2.104.3.3 Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.104.3.4 Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.104.3.5 Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.104.3.6 Comment

Enter a comment about this entry.

Console path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.104.4 Service list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

Console path:

Setup > **Bonjour-Proxy**

2.104.4.1 Name

Enter a name for this list here.

Console path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.104.4.2 Services

This table is used to specify the Bonjour service types that can be used in the services list.

Specify multiple services with a comma-separated list.

Console path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.104.5 Services

This table lists the default services for communicating between networks. You can extend the table according to your needs.

Console path:

Setup > **Bonjour-Proxy**

2.104.5.1 Name

Enter the service name here (e.g. "HTTP").

Console path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.5.2 Service type

Specify the service type here (e.g. `_http._tcp.local`).

Console path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.5.6 Comment

Enter a comment about this service.

Console path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.6 Query client

The table lists the services that should be requested by the router at regular intervals.

Console path:

Setup > **Bonjour-Proxy**

2.104.6.1 Name

Specify a unique name for the corresponding entry.

Console path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.6.2 Active

Enable or disable this entry.

Console path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

No
Yes

Default:

No

2.104.6.3 Server interface

Here you specify the server interface to be used for the client query.

Console path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.6.4 Services

Here you specify which services should be requested.

Console path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.104.7 Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

Console path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 4294967295

Default:

1024

2.104.8 Auto-query services

Activate the checkbox if the Query Client should periodically query the configured service types for their availability.

Console path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

Yes

2.105 OAM

Ethernet OAM according to 802.3ah is used by ISPs to monitor an Ethernet-based **last mile**, for example with FTTH or VDSL2 connections.

OAM packets (OAM Protocol Data Units or OAMPDUs) are regularly transmitted from the active side, which is usually the ISP side. The passive side, which is usually the CPE side, responds to these OAMPDUs. This is used to monitor the availability of the remote site. This procedure is known as **OAM discovery**.

Console path:

Setup

2.105.1 Interfaces

Specifies the OAM interfaces.

Console path:

Setup > **OAM**

2.105.1.1 Name

Name of the OAM interface.

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

16 characters from the following character set `[A-Z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

Default:

empty

2.105.1.2 Operating

Enables/disables OAM on the respective interface.

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Yes
No

Default:

No

2.105.1.3 Mode

Sets the mode for the interface.

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Active
The passive side (usually the CPE side) responds to the OAM packets (OAMPDUs) sent by the sender.

Passive
The active side (usually the internet provider) sends the OAM packets (OAMPDUs) to the receiver.

Default:

Passive

2.105.1.4 Remote-Loopback-Supported

Defines whether the device can be placed into loopback mode by the remote side. In loopback mode, the device disables forwarding and sends all received packets back on the interface. The packet is sent back exactly as it was received, without mirroring MAC or IP addresses.

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Yes
The device can be placed into loopback mode by the remote side.

No
The device cannot be placed into loopback mode by the remote side.

Default:

No

2.105.1.5 MIB-Retrieval-Supported

Defines whether the device allows the remote side to retrieve specific status values or counters from the device via packets.

Console path:

Setup > **OAM** > **Interfaces**

Possible values:

Yes

The device supports MIB retrieval.

No

The device does not support MIB retrieval.

Default:

No

2.105.3 CFM-Interfaces

This table defines the CFM parameters for the respective interface.

Console path:

Setup > **OAM**

2.105.3.1 Interface

Interface on which CFM should be activated. Possible values include LAN interfaces such as LAN-1 or WAN interfaces like DSL-1.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 18 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.105.3.2 MD-Level

Defines the Maintenance Domain Level for this interface.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

0 … 7

Default:

0

2.105.3.3 VLANs

Defines the VLANs on the interface with which CFM messages can be received and sent. Either a single VLAN or a comma-separated list of VLANs can be configured.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 50 characters from `[0-9],-/`

Default:

empty

Special values:

empty

All VLANs are accepted.

2.105.3.4 Operating

Enables or disables CFM on the configured interface.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No

CFM disabled.

Yes

CFM enabled.

Default:

No

2.105.3.5 Endpoint-Type

Defines the CFM endpoint type.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

MEP

The Maintenance Association End Point (MEP) represents the boundary of a domain and performs fault detection between the domain boundaries. The MEP creates and sends CFM packets.

MIP

The Maintenance Intermediate Point (MIP) is located within the domain and performs path and fault detection within the domain boundaries. The MIP responds to CFM packets.

Default:

MEP

2.105.3.6 Maintenance-Domain

Defines the name of the Maintenance Domain (MD).

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.105.3.7 Maintenance-Association

Defines the name of the Maintenance Association (MA).

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 45 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.105.3.8 MEPID

Defines the Maintenance Endpoint ID of the device for this entry. This must be unique on each device.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

1 … 8191

2.105.3.9 Sender-ID

Defines the optional sender ID in CFM-CCM messages.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.105.3.10 CoS

Defines the Class-of-Service with which CFM-CCM (Continuity Check Message) packets are marked.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

Best-Effort
Background
Excellent-Effort
Controlled-Latency
Video
Voice
Network-Control

Default:

Best-Effort

2.105.3.11 LBM-Responder

Defines whether the device should respond to CFM loopback messages (Ethernet ping). The function can be used independently of the CCM operating mode.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

2.105.3.21 LTM-Responder

Defines whether the device should respond to CFM linktrace messages (Ethernet traceroute). The function can be used independently of the CCM operating mode.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

2.105.3.31 CCM-Initiator

Defines whether the device should send regular CCM messages (Continuity Check Message).

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

2.105.3.32 CCM-Interval

Defines the interval at which CCM messages (Continuity Check Message) should be sent by the device. CCM intervals must be consistent between communication partners.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

3.333-msec
Interval of 3.333 milliseconds.

10-msec
Interval of 10 milliseconds.

100-msec
Interval of 100 milliseconds.

1-sec
Interval of one second.

10-sec
Interval of 10 seconds.

1-min
Interval of one minute.

10-min
Interval of 10 minutes.

Default:

3.333-msec

2.105.3.33 CCM-Lowest-Alarm-Prio

Defines the minimum severity level of detected faults required for the MEP to set the RDI (Remote Defect Indication) flag and propagate it in CCM packets. Levels, in ascending severity, are: RDICCM, MACstatus, RemoteCCM, ErrorCCM, XconCCM.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

RDICCM
A CCM frame with the RDI flag set was received from at least one other MEP.

MACstatus
At least one other MEP reported an interface status other than 'up' (e.g., hardware issue), or all other MEPs report a PortStatus other than 'up' (e.g., isolated network segment).

RemoteCCM
No CCM frames are received from at least one configured MEP.

ErrorCCM
Another MEP is using the same MEPID as the local device, or CCMs from an unconfigured MEP are received (if matching is not set to none), or another MEP is using a different CCM interval.

XconCCM
CCs were received from another MEP with a lower MD level or with a differing domain or association.

Default:

MACstatus

2.105.3.41 CCM-Receiver

Defines whether the device should process or receive CCM messages.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

No
Yes

Default:

No

2.105.3.42 Remote-MEP-Matching

Defines how the device should handle the presence of remote MEPs. Arbitrary remote MEPs can be dynamically learned, or it can be treated as an error if a configured remote MEP is not found.

Console path:

Setup > **OAM** > **CFM-Interfaces**

Possible values:

None

Unconfigured MEPs are added to the status table and are included in the RDICCM and MACstatus conditions.

Yes

Unconfigured MEPs are added to the status table but are not included in the RDICCM and MACstatus conditions. They trigger ErrorCCM.

Strict

Unconfigured MEPs are not added to the status table, are not included in the RDICCM and MACstatus conditions, and they trigger ErrorCCM.

Default:

None

2.105.4 Remote-Loopback

With this command, the device sends a Loopback Control OAMPDU to the counterpart, causing the counterpart to enter or exit the loopback mode accordingly. In loopback mode, the counterpart device sets the forwarding mode on this interface and returns all received packets. The packet is sent back exactly as it was received, without mirroring MAC or IP addresses.

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface on which to start or stop the loopback mode. The device sends the message on this interface to place the remote side into loopback mode or to terminate it there.

Possible values from the OAM setup table, e.g., LAN-1, DSL-1, …

[-?]

Displays brief help for the parameters.

<start|stop>

Starts or stops loopback mode.

2.105.5 Remote-MEPs

In this table, remote MEPs can optionally be defined that the device expects on the remote side.

Console path:

Setup > **OAM**

2.105.5.1 Maintenance-Domain

Defines the name of the Maintenance Domain (MD).

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

Max. 43 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.105.5.2 Maintenance-Association

Defines the name of the Maintenance Association (MA).

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

Max. 45 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

2.105.5.3 MEPID

Defines the Maintenance Endpoint ID of the device for this entry. This must be unique on each device.

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

1 … 8191

2.105.5.4 Remote-MEPID

Defines the remote MEPID expected for this configuration. This must be unique on each device.

Console path:

Setup > **OAM** > **Remote-MEPs**

Possible values:

1 … 8191

2.105.6 Variable-Read

This command allows the device to send a Variable Request OAMPDU to the remote side. The remote side responds with the value of the requested variable based on the local MIB. This method can be used to read packet counters on the remote side, for example. The remote side must support the feature of reading MIB variables via OAM.

Variables from IEEE 802.3.1 are supported, among others.

Example:

```
> do Variable-Read -i LAN-3 aFramesTransmittedOK

aFramesTransmittedOK = 8444
OK: Action Variable-Read done
```

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface from which the variable is to be read.

[-?]

Displays brief help for the parameters.

<variable name> [more variable names]

One or more variable names separated by spaces.

2.107 Automatic-Firmware-Update

The LANCOM Auto Updater allows on-site LANCOM devices to be updated automatically without further user intervention (unattended). LANCOM 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 LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

Console path:

Setup

2.107.1 Mode

Set the operating mode of the LANCOM 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 LANCOM update server for new updates. The availability of a new update is signaled to the user in the LCOS 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 LANCOM 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. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Default:

Check and update

2.107.2 Check firmware now

This command triggers the device to check the LANCOM 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 LANCOM 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 LANCOM 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: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security updates only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest 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 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 Rel.

Default:

Security updates only

2.107.9 Loopback-Addr.

A routing tag can be set automatically by specifying a loopback address.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

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:

Max. 2 characters from `[0-9]`

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:

Max. 2 characters from `[0-9]`

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:

Max. 2 characters from `[0-9]`

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:

Max. 2 characters from `[0-9]`

Default:

4

2.107.14 E-mail notification

This setting determines whether the LANCOM Auto Updater e-mail notifications are sent to the e-mail address specified in 2.107.15 . Administrators can use the e-mail notifications to receive information about events relating to the automatic firmware update by the Auto Updater. An e-mail is sent after the following events:

- An update was found (in the update mode “Check” only)
- An update was found and a time for automatic installation was scheduled (the in update mode “Check & Update”)
- An update has been successfully installed (including successful access check)
- An update was not successful and a fallback to the previously installed firmware was performed
- Error messages from the Auto Updater (e.g. update server could not be reached)

Notification is only given for automatically executed actions. If actions are started manually, e.g. an update check via LANmonitor or WEBconfig, then there is no e-mail notification.

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

No

The Auto Updater does not send notifications.

Yes

The Auto Updater sends notifications.

Default:

No

2.107.15 E-mail address

Here you can enter the e-mail address to be used by the LANCOM Auto Updater when e-mail alerts are enabled under 2.107.14 .

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.108 Multicast

This item contains the settings for multicast protocols.

Console path:

Setup

2.108.1 IGMP

This item contains the settings for the Internet Group Management Protocol (IGMP).

Console path:

Setup > **Multicast**

2.108.1.1 IGMP-Proxy

An IGMP proxy is typically used for Internet connections with multicast IPTV. Clients or IPTV set top boxes (STBs) on the local network send IGMP messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or IGMP proxy receives the IGMP messages and forwards them to the provider network and filters the groups, if required. The IGMP proxy works for the local network with its clients.

An IGMP proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the IGMP proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. IGMP proxies can be “cascaded” by connecting multiple routers in series.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.1.1 Downstream-Interface

Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Possible values are IPv4 networks, e.g. INTRANET, IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. “VPN*”.

Console path:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.1.2 Upstream-Interface

Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Console path:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.1.3 Group-Filter

Name of the group filter that is to apply to this proxy. References the table *IPv4 filter table*. By default, the filter entry is blank or points to the filter list “ANY”, which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

Console path:

Setup > **Multicast** > **IGMP** > **IGMP-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.1.3 SSM-Ranges

Specifies the IP address range in prefix notation used for SSM.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.3.1 Prefix

These prefixes define the IPv4 address range used for SSM.

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Ranges**

Possible values:

Max. 18 characters from `[0-9]./`

2.108.1.4 SSM-Source-IP-List

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.4.1 Name

Enter a name for the entry. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Source-IP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.1.4.2 IP-Address

Unicast source IP address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

Console path:

Setup > **Multicast** > **IGMP** > **SSM-Source-IP-List**

Possible values:

Max. 15 characters from `[0-9].`

2.108.1.5 Static-Routes

Static multicast routing can be used where multicast clients do not support IGMP and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates IGMP joins and group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.5.1 Upstream-Interface

Interface name where the multicast packets reach the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.5.2 Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. 239.0.0.1.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Max. 15 characters from `[0-9].`

2.108.1.5.3 Downstream-Interface

Interface name where the multicast packets exit the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.5.4 Mode

If SSM is to be operated: This controls the way in which an IGMP membership report requests the source addresses of multicast sources.

If you want to use an SSM group with any source address, you have to link the mode “Exclude” and SSM source IP list “ANY”.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Include

An IGMP membership report is sent with the record type “Change to Include Mode”. The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting “Include” and the SSM source IP list with an entry “ANY” will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An IGMP membership report is sent with the record type “Change to Exclude Mode”. If the source list contains the entry “ANY” or “0.0.0.0”, i.e. all sources are allowed, then an IGMP membership report will be sent with a join group for “any sources”. If the list contains an entry other than 0.0.0.0, an IGMP membership report “block sources” is sent with the corresponding IP address.

2.108.1.5.5 SSM-Source-IP-List

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list “ANY” can be used with the entry “0.0.0.0”.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.1.6 Parameter

The settings for the general IGMP parameters are located here.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.6.1 Interface

Name of the interface that the IGMP configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv4 networks, e.g. INTRANET or IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. “VPN*”.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.6.2 Robustness-Variable

Number of IGMP message repeats.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.1.6.3 Unsolicited-Report-Interval

Specifies the time in seconds between repetitions of a host's initial report of membership in a group.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 25

Default:

2

2.108.1.6.4 Query-Interval

Interval between IGMP general queries.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

2 … 99999

Default:

125

2.108.1.6.5 Query-Response-Interval

Maximum response time in milliseconds. The maximum response time is inserted into periodic general queries. The value for the query response interval must be less than the value for query interval.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 999999

Default:

10000

2.108.1.6.6 Startup-Query-Interval

The interval in seconds between IGMP general queries sent after the querier starts up.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 99998

Default:

30

2.108.1.6.7 Startup-Query-Count

Number of IGMP general queries sent on startup, separated by the startup query interval.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.1.6.8 Last-Listener-Query-Interval

Specifies the value in seconds of the Maximum Response Time in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 25

Default:

2

2.108.1.6.9 Last-Listener-Query-Count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.1.6.10 IGMP-Compatibility-Mode

IGMP version used by the device when operating as a multicast router.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

Off
V1
V2
V3

Default:

V3

2.108.1.6.11 Quick-Leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms.

Console path:

Setup > **Multicast** > **IGMP** > **Parameter**

Possible values:

No
Yes

Default:

No

2.108.1.7 Check-Router-Alert

Defines whether received IGMP messages are checked for the Router Alert option. According to RFC, IGMP packets that do not contain the Router Alert option should be discarded. This is designed to ensure compatibility in case of faulty client implementations.

Console path:

Setup > **Multicast** > **IGMP**

Possible values:

No
Yes

Default:

Yes

2.108.1.8 Collect-Statistics

Defines whether IPv4 multicast statistics should be collected. Collecting these statistics may affect device performance.

Console path:

Setup > **Multicast** > **IGMP**

Possible values:

No
Yes

Default:

No

2.108.1.9 Static-Join

This table is used to define IPv4 multicast groups that the device can join through IGMP in order to test client interfaces. This allows the simulation of multicast clients joining certain IGMP groups. The corresponding client interface must be part of the IGMP proxy or PIM configuration. The device then processes and discards inbound multicast traffic. This feature is not suitable for permanent operation in productive scenarios.

Console path:

Setup > **Multicast** > **IGMP**

2.108.1.9.1 Interface

(Client) interface name used to simulate the multicast client.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Join**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.1.9.2 Group

IPv4 multicast group that the device joins statically.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Join**

Possible values:

Max. 15 characters from `[0-9].`

2.108.1.9.3 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **IGMP** > **Static-Join**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.2 MLD

This item contains the settings for the Multicast Listener Discovery (MLD).

Console path:

Setup > **Multicast**

2.108.2.1 MLD-Proxy

An MLD proxy is typically used for multicast IPTV on IPv6 Internet connections. Clients or IPTV set top boxes (STBs) on the local network send MLD messages to receive a specific TV channel. To this end, they join certain multicast groups

and later leave them again. The router and/or MLD proxy receives the MLD messages and forwards them to the provider network and filters the groups, if required. The MLD proxy works for the local network with its clients.

An MLD proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the MLD proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. MLD proxies can be "cascaded" by connecting multiple routers in series.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.1.1 Downstream-Interface

Interface name used by MLD clients to join groups and receive MLD messages from the proxy. Possible values are IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or RAS templates.

Console path:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.1.2 Upstream-Interface

Interface name used by the MLD proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Console path:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.1.3 Group-Filter

Name of the group filter that is to apply to this proxy. References the table *IPv6 filter table*. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

Console path:

Setup > **Multicast** > **MLD** > **MLD-Proxy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.3 SSM-Ranges

Specifies the IP address range in prefix notation used for SSM.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.3.1 Prefix

These prefixes define the IP address range used for SSM.

Console path:

Setup > **Multicast** > **MLD** > **SSM-Ranges**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

2.108.2.4 SSM-Source-IP-List

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.4.1 Name

Enter a name for the entry. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **MLD** > **SSM-Source-IP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.4.2 IP-Address

Unicast source IP address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

Console path:

Setup > **Multicast** > **MLD** > **SSM-Source-IP-List**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.108.2.5 Static-Routes

Static multicast routing can be used where multicast clients do not support MLD and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates MLD group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.5.1 Upstream-Interface

Interface name where the multicast packets reach the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.5.2 Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. “ff09::1”.

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.108.2.5.3 Downstream-Interface

Interface name where the multicast packets exit the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.5.4 Mode

If SSM is to be operated: This controls the way in which an MLD membership report requests the source addresses of multicast sources.

If you want to use an SSM group with any source address, you have to link the mode “Exclude” and SSM source IP list “ANY”.

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Include

An MLD membership report is sent with the record type “Change to Include Mode”. The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting “Include” and the SSM source IP list with an entry “ANY” will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An MLD membership report is sent with the record type “Change to Exclude Mode”. If the source list contains the entry “ANY” or “0.0.0.0”, i.e. all sources are allowed, then an MLD membership report will be sent with a join group for “any sources”. If the list contains an entry other than 0.0.0.0, an MLD membership report “block sources” is sent with the corresponding IP address.

2.108.2.5.5 SSM-Source-IP-List

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list “ANY” can be used with the entry “0.0.0.0”.

Console path:

Setup > **Multicast** > **MLD** > **Static-Routes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.2.6 Parameter

The settings for the general MLD parameters are located here.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.6.1 Interface

Name of the interface that the MLD configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or IPv6 RAS templates.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.2.6.2 Robustness variable

Number of MLD message repeats.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.2.6.3 Unsolicited-Report-Interval

Specifies the time in seconds between repetitions of a host's initial report of membership in a group.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 25

Default:

2

2.108.2.6.4 Query-Interval

Interval in seconds between MLD general queries.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

2 … 99999

Default:

125

2.108.2.6.5 Query-Response-Interval

The maximum response time is inserted into periodic MLD general queries. The value for the query response interval must be less than the value for query interval.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 999999

Default:

10000

2.108.2.6.6 Startup-Query-Interval

The interval in seconds between MLD general queries sent after the MLD querier starts up.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 99998

Default:

30

2.108.2.6.7 Startup-Query-Count

Number of MLD general messages on startup, separated by the startup query interval.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.2.6.8 Last-Listener-Query-Interval

Specifies the value in seconds of the Maximum Response Code (with IPv6) in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 25

Default:

2

2.108.2.6.9 Last-Listener-Query-Count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

1 … 10

Default:

2

2.108.2.6.10 MLD-Compatibility-Mode

MLD version used by the device when operating as a multicast router.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

Off
V1
V2

Default:

V2

2.108.2.6.11 Quick-Leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms.

Console path:

Setup > **Multicast** > **MLD** > **Parameter**

Possible values:

No
Yes

Default:

No

2.108.2.8 Collect-Statistics

Defines whether IPv6 multicast statistics should be collected. Collecting these statistics may affect device performance.

Console path:

Setup > **Multicast** > **MLD**

Possible values:

No
Yes

Default:

No

2.108.2.9 Static-Join

This table is used to IPv6 multicast groups that the device can join through MLD for in order to test client interfaces. This allows the simulation of multicast clients joining certain MLD groups. The corresponding client interface must be part of the IGMP proxy or PIM configuration. The device then processes and discards inbound multicast traffic. This feature is not suitable for permanent operation in productive scenarios.

Console path:

Setup > **Multicast** > **MLD**

2.108.2.9.1 Interface

(Client) interface name used to simulate the multicast client.

Console path:

Setup > **Multicast** > **MLD** > **Static-Join**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.2.9.2 Group

IPv6 multicast group that the device joins statically.

Console path:

Setup > **Multicast** > **MLD** > **Static-Join**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.108.2.9.3 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **MLD** > **Static-Join**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.2.127 Enable-Lancom-Group

Specifies whether the device should respond to the multicast address ff02::139. This multicast group is used by the LANtools to find LANCOM devices.

Console path:

Setup > **Multicast** > **MLD**

Possible values:

No
Yes

Default:

Yes

2.108.4 PIM

This item contains the settings for PIM (Protocol Independent Multicast).

Console path:

Setup > **Multicast**

2.108.4.1 IPv4

This item contains the settings for PIM (Protocol Independent Multicast) with IPv4.

Console path:

Setup > **Multicast** > **PIM**

2.108.4.1.1 RP-List

In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.

Console path:

Setup > **Multicast** > **PIM** > **IPv4**

2.108.4.1.1.1 Group-Filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 1865 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.1.1.2 Rtg-Tag

The routing tag used to reach this rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-List**

Possible values:

0 … 65535

Default:

0

2.108.4.1.1.3 RP-Address

IPv4 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-List**

Possible values:

Max. 15 characters from `[0-9].`

2.108.4.1.1.5 RP-Name

Name of the rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.4.1.1.6 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **RP-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.108.4.1.2 SSM-List

This table configures the parameters for PIM SSM (Source Specific Multicast) mode.

Console path:

Setup > **Multicast** > **PIM** > **IPv4**

2.108.4.1.2.1 Group-Filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 1865 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.1.2.2 Rtg-Tag

Routing tag to which this configuration applies.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-List**

Possible values:

0 … 65535

Default:

0

2.108.4.1.2.3 SSM-Source-Filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the *2.108.4 PIM* on page 1853 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.1.2.5 SSM-Name

Name of this SSM configuration.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.4.1.2.6 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.4.1.3 SSM-Mapping

In this table, IPv4 multicast source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses (S) in received IGMP messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.

Console path:

Setup > **Multicast** > **PIM** > **IPv4**

2.108.4.1.3.1 Group-Filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the *2.108.5 IPv4-Filter-Table* on page 1865 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Mapping**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.1.3.2 Rtg-Tag

Routing tag to which this configuration applies.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Mapping**

Possible values:

0 … 65535

Default:

0

2.108.4.1.3.3 SSM-Source-IP

Specifies a source IPv4 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Mapping**

Possible values:

Max. 15 characters from `[0-9].`

2.108.4.1.3.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv4** > **SSM-Mapping**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.4.2 IPv6

This item contains the settings for PIM (Protocol Independent Multicast) with IPv6.

Console path:

Setup > **Multicast** > **PIM**

2.108.4.2.1 RP-List

In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.

Console path:

Setup > **Multicast** > **PIM** > **IPv6**

2.108.4.2.1.1 Group-Filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 1866 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.2.1.2 Rtg-Tag

The routing tag used to reach this rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-List**

Possible values:

0 … 65535

Default:

0

2.108.4.2.1.3 RP-Address

IPv6 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-List**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.108.4.2.1.5 RP-Name

Name of the rendezvous point.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.4.2.1.6 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **RP-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

2.108.4.2.2 SSM-List

This table configures the parameters for PIM IPv6 SSM (Source Specific Multicast) mode.

Console path:

Setup > **Multicast** > **PIM** > **IPv6**

2.108.4.2.2.1 Group-Filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 1866 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.2.2.2 Rtg-Tag

Routing tag to which this configuration applies.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-List**

Possible values:

0 … 65535

Default:

0

2.108.4.2.2.3 SSM-Source-Filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the *2.108.1.4 SSM-Source-IP-List* on page 1837 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.2.2.5 SSM-Name

Name of this SSM configuration.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.108.4.2.2.6 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.4.2.3 SSM-Mapping

In this table, IPv6 source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses in received MLD messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.

Console path:

Setup > **Multicast** > **PIM** > **IPv6**

2.108.4.2.3.1 Group-Filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the *2.108.6 IPv6-Filter-Table* on page 1866 table.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Mapping**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.4.2.3.2 Rtg-Tag

Routing tag to which this configuration applies.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Mapping**

Possible values:

0 … 65535

Default:

0

2.108.4.2.3.3 SSM-Source-IP

Specifies a source IPv6 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Mapping**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.108.4.2.3.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **PIM** > **IPv6** > **SSM-Mapping**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.4.3 Interfaces

This table specifies the interfaces and logical networks where PIM is to be enabled. It also specifies the interfaces where clients can join multicast groups by means of IGMP or MLD.

Console path:

Setup > **Multicast** > **PIM**

2.108.4.3.1 Interface

Name of the logical interface on which PIM or a GMP (group management protocol such as IGMP or MLD) is to be activated. Possible values are IPv4 networks, e.g. INTRANET, WAN remote sites, wildcard entries with * for IPv4 RAS interfaces, for example "VPN*". Other possible values are IPv6 interfaces and IPv6 RAS templates.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.108.4.3.2 PIM-Active

Enables PIM as well as sending and receiving PIM messages on this logical interface. If this interface is only used by IGMP/MLD clients or multicast recipients, sending and receiving PIM messages can be explicitly disabled. In this case, only GMP (IGMP/MLD) has to be activated.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

No

PIM is disabled.

Yes

PIM is enabled.

2.108.4.3.3 GMP-Active

Enables the IGMP or MLD router role on this logical interface. In this case, IGMP or MLD joins from clients are accepted. GMP can be disabled on interfaces where the network contains no clients but only PIM neighbor routers. IGMP/MLD joins will not be accepted in this case.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

No

IGMP or MLD router role is disabled.

Yes

IGMP or MLD router role is enabled.

2.108.4.3.4 Address-Type

Here you specify the address family for which PIM or GMP should be enabled on this interface.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

IPv4
IPv6

2.108.4.3.5 Hello-Interval

Sets the time in seconds between the repetition of regular PIM Hello messages. The hold time is automatically 3.5 times the PIM Hello interval and cannot be configured separately.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

0 … 255

Default:

30

Special values:

0

The value 0 disables the sending of Hello messages.

2.108.4.3.6 DR-Priority

Specifies the priority as designated router (DR) in the DR election process in PIM. A higher value means a higher priority in the DR election. If several routers have the same (highest) priority, the router with the highest numeric IP address will be the DR.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

0 … 4294967296

Default:

1

2.108.4.3.7 Tracking-Support

Affects the “T bit” setting in the LAN Prune Delay option in outgoing Hello messages.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

Yes
Off

Default:

Off

2.108.4.3.8 Override-Interval

Affects the setting of the override interval field in the LAN Prune Delay option in outgoing Hello messages. Specifies the maximum delay for transmitting Override Join messages for multicast networks that have Join-Suppression enabled.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

0 … 4294967296

Default:

0

2.108.4.3.9 Propagation-Delay

Configures the setting of the Propagation Delay field in Hello messages sent for the LAN Prune Delay option. Specifies the delay in milliseconds for implementing a PIM prune message on the upstream routing device on a multicast network for which join suppression has been enabled.

Console path:

Setup > **Multicast** > **PIM** > **Interfaces**

Possible values:

250 … 2000

Default:

500

2.108.4.6 Operating

Enables or disables PIM on the device.

Console path:

Setup > **Multicast** > **PIM**

Possible values:

No

PIM is disabled.

Yes

PIM is enabled.

Default:

No

2.108.5 IPv4-Filter-Table

This table can be used to specify lists of desired or unwanted IPv4 multicast addresses and prefixes.

These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast**

2.108.5.1 Name

Give this entry a name. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.5.2 Prefix

Enter here the IPv4 address followed by the prefix length of the network (CIDR notation). This specifies how many most-significant bits (MSB) of the IP address are necessary for a match.

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Max. 18 characters from `[0-9]./`

2.108.5.3 Action

Specify whether the prefixes in this filter entry should be allowed or denied.

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Allow
Deny

2.108.5.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **IPv4-Filter-Table**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.108.6 IPv6-Filter-Table

This table can be used to specify lists of desired or unwanted IPv6 multicast addresses and prefixes.

These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast**

2.108.6.1 Name

Give this entry a name. A list is defined by several entries with the same name.

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

2.108.6.2 Prefix

Enter the IPv6 multicast address and prefix here.

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

2.108.6.3 Action

Specify whether the prefixes in this filter entry should be allowed or denied.

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Allow
Deny

2.108.6.4 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **Multicast** > **IPv6-Filter-Table**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.109 NetFlow

NetFlow is a feature that allows network devices such as routers or switches to export information about their inbound and outbound IP traffic. The so-called IP flows are transmitted by UDP. An IP flow contains information about the source IP address, destination IP address, ports, timestamp and packet counters, among others. This information is received, stored and processed on a NetFlow collector. NetFlow can be used either permanently or temporarily for network analysis.

LANCOM supports the standards NetFlow 9 (*RFC 3954*) as well as IPFIX (*RFC 7011*), which is an extension of NetFlow Version 9, via the transport protocol UDP.

Notes on use:

- You need an external NetFlow collector that supports NetFlow 9 or IPFIX.
- The firewall must be activated.
- The only flow information collected with IPv4 is that being passed from one logical interface to another logical interface. Packets generated by or addressed to the router itself are not captured. For IPv6, this restriction does not apply.
- Only unicast IP flow information is collected, multicast (e.g. IPTV) is not supported.

› Depending on the scenario, using NetFlow/IPFIX increases CPU load and reduces the overall performance of the router.

Console path:

Setup

2.109.1 Collectors

Configure the collectors for NetFlow/IPFIX here.

Console path:

Setup > **NetFlow**

2.109.1.1 Name

Unique name of the NetFlow collector. This name is referenced in other tables.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.1.2 Address

IPv4, IPv6 address or host name of the collector.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.1.3 Port

NetFlow collector port. Usually port 2055 for NetFlow 9 and 4739 for IPFIX.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 5 characters from `[0-9]`

2.109.1.4 Protocol

Protocol version used by the NetFlow collector.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

IPFIX-UDP
NetFlow9-UDP

2.109.1.5 Loopback-Addr.

Optionally, specify a source address.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.1.6 Rtg-Tag

Specify a routing tag if a particular route is to be used to the collector.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

0 … 65535

Default:

0

2.109.1.7 Template-Refresh-Time

Specifies the time in minutes after which a NetFlow template record is refreshed. The value 0 deactivates the periodic refresh of template records.

A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 5 characters from `[0-9]`

2.109.1.8 Template-Refresh-Packets

Specifies the number of packets after which a NetFlow template record is refreshed. The value 0 deactivates the refresh of template records based on a packet counter.

A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 10 characters from `[0-9]`

2.109.1.99 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **NetFlow** > **Collectors**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.109.2 Interfaces

Configure the interfaces for NetFlow/IPFIX here.

Console path:

Setup > **NetFlow**

2.109.2.1 Ifc

Logical interface on which NetFlow/IPFIX is to be activated. Possible values: IPv4, IPv6 LAN interfaces, remote sites, IPv6 RAS template. IPv4 remote sites can use a wildcard, e.g. Company*

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.109.2.2 Collector

This references an entry in the list of collectors.

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.2.3 Active

Enables/disables NetFlow/IPFIX for this entry for the interface and the collector.

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Yes

NetFlow/IPFIX is enabled for this interface.

No

NetFlow/IPFIX is disabled for this interface.

2.109.2.4 Metering-Profile

This references an entry in the list of metering profiles.

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.2.99 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **NetFlow** > **Interfaces**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.109.3 Operating

Enable NetFlow/IPFIX on the device.

Console path:

Setup > **NetFlow**

Possible values:

Yes

NetFlow/IPFIX is enabled.

No

NetFlow/IPFIX is disabled.

2.109.4 Metering-Profiles

Configure the profiles for NetFlow/IPFIX here.

Console path:

Setup > **NetFlow**

2.109.4.1 Name

Unique name of the metering profile. This name is referenced in other tables.

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

Max. 20 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.109.4.2 Direction

IP flow direction to be monitored by NetFlow/IPFIX.

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

Ingress

Inbound IP data streams from the perspective of NetFlow/IPFIX.

Egress

Outbound IP streams from the perspective of NetFlow/IPFIX.

All

Inbound and outbound IP data streams.

2.109.4.3 IP-Version

IP protocol version(s) to be monitored by NetFlow/IPFIX.

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

IPv4
IPv6
All

2.109.4.99 Comment

Optionally enter a meaningful comment as a description.

Console path:

Setup > **NetFlow** > **Metering-Profiles**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.109.5 Active-Flow-Timeout

Defines the interval in seconds after a running data stream is exported via Netflow. This makes it possible to run longer sessions, e.g. to export large downloads at runtime. Subsequent traffic is classified as a new data flow, and the logging of the data traffic by the collector starts again.

Console path:

Setup > **NetFlow**

Possible values:

60 … 1800 Seconds

Special values:

0

Switched off

Default:

1800

2.110 Firewall

Firewall settings

Console path:

Setup

2.110.2 DNS-Destination-List

In the DNS destination list, you can group multiple DNS destinations into one referenced object.

Console path:

Setup > **Firewall**

2.110.2.1 Name

The name for this DNS destination list. This name is used to reference this object.

Console path:

Setup > **Firewall** > **DNS-Destination-List**

Possible values:

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.110.2.2 Targets

Contains a comma-separated or space-separated list of names of the DNS destinations.

Console path:

Setup > **Firewall** > **DNS-Destination-List**

Possible values:

Max. 252 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.110.3 DNS minimum cache time

This option specifies the minimum time in seconds that a DNS entry is stored if the TTL in the DNS packet is less than the configured value. A buffer of 10 seconds is added. The value that is taken is the maximum of this parameter **DNS minimum cache time** and the TTL from the DNS packet plus 10 seconds.

Console path:

Setup > **Firewall**

Possible values:

Max. 11 characters from `[0-9]`

Default:

180

2.110.4 Dynamic-Path-Selection

Used in an SD-WAN scenario where several lines are available, Dynamic Path Selection optimizes the application performance by directing the data traffic over the line with the best quality according to metrics such as load, packet loss, latency or jitter.

Dynamic Path Selection is activated on a load balancer (see *2.8.10.2.16 LB-Policy* on page 232). A load balancer can be defined either for Internet connections or for SD-WAN overlay tunnels (VPN). The end point for ICMP test packets can either be any IP address or the central-site SD-WAN gateway.

Console path:

Setup > **Firewall**

2.110.4.1 ICMP-Measurement-Profiles

ICMP measurement profiles specify a parameter set used by measurements that are based on ICMP pings. Interface metrics are derived from measurements to quantify the connection quality. These metrics are: Average round trip time (RTT, latency), jitter and packet loss rate.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.1.1 Measurement-Profile

The name of the profile. This name is used to reference the profile in DPS policies.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.2 DSCP-value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

BE
CS0
CS1
CS2
CS3
CS4
CS5
CS6
CS7
AF11
AF12
AF13
AF21
AF22
AF23
AF31
AF32
AF33
AF41
AF42
AF43
EF

2.110.4.1.3 Loopback-Addr.

Optionally references a named loopback address used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.4 IPv4-Destination-1

The first of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With "0.0.0.0" entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.5 IPv6-Destination-1

The first of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.6 Payload-Size

Specifies the size of the data payload that follows the ICMP header (payload size) of the pings being sent.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.1.7 Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.1.8 Sliding-Window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.1.9 IPv4-Destination-2

The second of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With “0.0.0.0” entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.10 IPv4-Destination-3

The third of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With “0.0.0.0” entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.11 IPv4-Destination-4

The first of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With “0.0.0.0” entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.12 IPv6-Destination-2

The second of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.13 IPv6-Destination-3

The third of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.14 IPv6-Destination-4

The fourth of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.1.15 Unit

Specifies whether the ICMP measurements for the value should be in seconds or milliseconds.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **ICMP-Measurement-Profiles**

Possible values:

Seconds
Milliseconds

Default:

Seconds

2.110.4.2 HTTP-Measurement-Profiles

HTTP measurement profiles specify a parameter set used by measurements that are based on HTTP(S) connections. Interface metrics are derived from measurements that quantify the connection quality. These metrics are: Mean time to establish an HTTP(S) connection (latency), jitter, and connection-error rate (packet loss).

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.2.1 Measurement-Profile

The name of the profile. This name is used to reference the profile in DPS policies.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.2 DSCP value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

BE
CS0
CS1
CS2
CS3
CS4
CS5
CS6
CS7
AF11
AF12
AF13
AF21
AF22
AF23
AF31
AF32
AF33
AF41
AF42
AF43
EF

2.110.4.2.3 Loopback-Addr.

Optionally references a named loopback address used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.4 IPv4-Destination-1

The first of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With “0.0.0.0” entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.5 IPv6-Destination-1

The first of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.6 Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.2.7 Sliding-Window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.2.8 IPv4-Destination-2

The second of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With “0.0.0.0” entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.9 IPv4-Destination-3

The third of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With “0.0.0.0” entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.10 IPv4-Destination-4

The fourth of up to 4 measurement targets as a valid IPv4 unicast address or DNS host name. With “0.0.0.0” entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.11 IPv6-Destination-2

The second of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.12 IPv6-Destination-3

The third of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.2.13 IPv6-Destination-4

The fourth of up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **HTTP-Measurement-Profiles**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.16 Policies

To evaluate the connection quality of the interfaces used for Dynamic Path Selection, the metrics calculated from the measurement profiles are compared to threshold values, and points (as a score) are awarded. These points added up to determine which is the “best” interface. Certain thresholds can be specified as being “critical” (e.g. jitter <= 30 ms). Dynamic load balancer decisions are based on the points total in combination with the exceeded critical threshold values. A DPS policy collects the threshold values and criticality markings that are required to calculate the total points.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.16.1 Policy

The name of the DPS policy. This name is used to reference the policy in firewall rules. All of the rows in this table with the same policy name are combined into one policy. This makes it possible, for instance, to use the same metric multiple

times with different thresholds in the same policy. This allows a points-based grading (e.g. 10 points with a latency <= 100, another 10 points with a latency <= 50).

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.16.2 Measurement-Profile

Either empty or the name of an ICMP measurement profile.

The field must be empty if, and only if, the SLA metric “Load(%)” is selected. In all other cases, a measurement profile must be specified.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.16.3 SLA-Metric

This is the metric generated from the measurements of the set measurement profile. The value of metric is compared to the threshold value.

The metric “Load(%)” denotes the utilization of the interface in percent of the maximum bandwidth. As this value is not determined using separate measurements, the entry *2.110.4.16.2 Measurement-Profile* on page 1884 must be left empty.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

Latency (ms)
Jitter (ms)
Packet loss (%)
Load (%)

2.110.4.16.4 Threshold

Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements need to be prevented by making an an exception for this interface in all of the affected policies.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

Max. 10 characters from `[0-9]`

2.110.4.16.5 Value

If a metric undershoots the chosen threshold, the points are added to the overall result of the policy.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

Max. 5 characters from `[0-9]`

2.110.4.16.6 Critical

Marks whether a threshold is critical. If a threshold value marked as “critical” is not undershot, the overall result is not defined.

An interface with an undefined overall result cannot be selected by a dynamic load balancer decision.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policies**

Possible values:

No

Threshold is not marked as critical.

Yes

Threshold is marked as critical.

2.110.4.17 Policy-Assignments

Here you set which DPS policy should be used with which load balancer, and what the priorities are if the overall results are equal.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.17.1 Policy

The name of an existing DPS policy from *2.110.4.16.1 Policy* on page 1883.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.2 Load-Balancer

Name of a load balancer (*2.8.20.2.1 Peer* on page 254) to be rated by this policy. Measurements are automatically started on all interfaces of this load balancer according to the measurement profiles referenced in the policy.

Measurements can be suppressed for individual interfaces of this load balancer. See also *2.110.4.18 Policy-Assignment-Exceptions* on page 1887.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.3 Priority-1

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.4 Priority-2

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.5 Priority-3

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.6 Priority-4

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.17.7 Switchover-Profile

The name of a switchover profile to be used for this policy. Also see *2.110.4.32.1 Switchover-Profile* on page 1889.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignments**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.18 Policy-Assignment-Exceptions

One option is not to apply measurement profiles to certain interfaces, for example if they are charged by data volume.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.18.1 Policy

The name of an existing DPS policy from *2.110.4.16.1 Policy* on page 1883.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignment-Exceptions**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.18.2 Interface

The name of an interface (e.g. WAN remote sites, VPN tunnels) belonging to a load balancer that is rated by the policy. The measurement profiles referenced in the policy are not used to start measurements on the interface.

Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements must be prevented by making an an exception for this interface in all of the affected policies.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignment-Exceptions**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.18.3 Score-Fixed

Since no dynamic overall result can be derived without making measurements, this score for the interface is used for all decisions relating to dynamic path selection.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Policy-Assignment-Exceptions**

Possible values:

Max. 10 characters from `[0-9]`

2.110.4.32 Switchover-Profiles

By default, Dynamic Path Selection only distributes new sessions to a better line. If you want ongoing sessions to be shifted to a better line, you have to enable session switchover. A session switchover only makes sense for unmasked connections, such as VPN or SD-WAN overlays. With masked connections, the public WAN address would change during the session, so it would be rejected by servers offering SIP sessions or online banking. Two configuration steps are necessary to enable session switchover:

1. The firewall rules for Dynamic Path Selection must have session switchover enabled
2. A switchover profile must be linked to the corresponding policy in the Policy assignments table

The switchover profile can be used to control how quickly the set of sessions is moved to the new line or interface on the same load balancer.

To prevent sessions from being concentrated on a single interface, sessions are usually moved step-by-step in groups within the configured timeframe. Before each step, a check sees whether the switchover is still necessary, because in the meantime the policy scores and thus the ranking of the interfaces may have changed. If it is no longer necessary, switchover is canceled and the sessions remain on their current interface. If it remains necessary, the sessions for the group being moved in the next step are determined at random.

If the number of steps = 1 or the overall time = 0, all of the sessions are moved immediately.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection**

2.110.4.32.1 Switchover-Profile

The name of the switchover profile. This name is used to reference the profile.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Switchover-Profiles**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.110.4.32.2 Steps

Number of steps or groups in which the set of sessions is moved to the new line.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Switchover-Profiles**

Possible values:

Max. 2 characters from `[0-9]`

2.110.4.32.3 Timeframe(s)

Timeframe in seconds within which the set of sessions is shifted to the new line.

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Switchover-Profiles**

Possible values:

Max. 4 characters from `[0-9]`

2.110.4.32.4 Regard-LB-Prio

This parameter controls the behavior of the DPS session switchover.

If the table is reset to the default, the row "AGGRESSIVE-SWITCHOVER" is set to "Yes" and "SOFT-SWITCHOVER" is set to "No".

Console path:

Setup > **Firewall** > **Dynamic-Path-Selection** > **Switchover-Profiles**

Possible values:

Yes

Sessions also switch between interfaces with the same score, provided that the prioritization specified in table *2.110.4.17 Policy-Assignments* on page 1885 favors one of them. In this case, the output tables **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv4-Preferred-Lines-Log** and **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv6-Preferred-Lines-Log** will only show the highest-priority interface as "Preferred". This is also the interface that all sessions switch over to, with a speed and with the

number of intermediate steps as determined by the other parameters in the corresponding switchover profile.

This setting is useful in the following scenario, an an example: LTE or 5G is used together with VDSL. In some locations, LTE/5G is significantly faster than VDSL. For cost reasons, however, DSL should be used first instead of LTE/5G, since this should only be used as a booster. This also works with the priorities of the load balancer, for example. With the default behavior, however, the switchover does not switch back from the bad line to the better one.

This is the default for new entries.

No

The DPS session switchover is only performed if another line is actually better (higher score) than the line currently used by the session. Not taken into account is the prioritization that can be entered into the load balancer policy assignments. For this reason there are no switch-overs between interfaces with identical policy scores.

This is the default for entries from before LCOS 10.80.

Default:

Yes

2.110.5 BPJM

Settings of the BPjM module.

Console path:

Setup > **Firewall**

2.110.5.1 BPJM-Loopback-Address

Loopback address used by the BPjM module to access the server for BPjM signature updates.

Console path:

Setup > **Firewall** > **BPJM**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.111 IoT

Settings for IoT technologies supported by LCOS, such as Wireless ePaper, iBeacon and Bluetooth Low Energy.

Console path:

Setup

2.111.88 Wireless-ePaper

Configure the settings for the Wireless ePaper module here.

Console path:

Setup > **IoT**

2.111.88.1 Operating

This entry allows you to set the operating mode of the module.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No

The module is not enabled.

Manual

Wireless ePaper configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Manual

2.111.88.2 Port

Assign a port to the Wireless ePaper module. If the connection is initiated by the Wireless ePaper Server, the default port is 7533. If TLS is used and the connection is initiated by the Wireless ePaper device, set the port to 7534.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

Max. 5 characters from `[0-9]`

Default:

7353

2.111.88.3 Channel

Set which channel the Wireless ePaper module should use.

If you need to *coordinate the channel selection* due to several APs being within range of one another, you should select automatic channel selection here.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:

2425MHz

2.111.88.4 Channel-Coordination

Prevents collisions on ePaper channels due to APs within range of each other.

Console path:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.4.1 Operating

The coordinated channel selection is activated or deactivated here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0
No

1
Yes

Default:

1

2.111.88.4.2 Network

Here you specify the network that the access points are to use to communicate with each other.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

16 characters from the following character set `[A-Z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

2.111.88.4.3 Announce-address

Set the announce address here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

39 characters from the following character set: `[0-9 A-F a-f :.]`

2.111.88.4.4 Announce-port

Set the announce port here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.111.88.4.5 Announce-interval

Set the announce interval here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.111.88.4.6 Announce-timeout-factor

Set the announce timeout factor here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.111.88.4.7 Announce-timeout-interval

Set the announce timeout interval here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.111.88.4.8 Announce-master-backoff-interval

Set the announce master backoff interval here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

2.111.88.4.9 Coordination-port

Set the coordination port here.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

2.111.88.4.10 Coordination-keep-alive-interval

Here you set the coordination keep-alive interval.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.111.88.4.11 Coordination-reconnect-interval

Here you set the coordination reconnect interval.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

2.111.88.4.12 Assignment-switch-threshold

Here you set the assignment switch threshold.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

2.111.88.4.13 Distance-weighting

Here you set the weighting of WLAN distance.

A higher value means a better weighting.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

2.111.88.4.14 Channel-weighting

Here you set the weighting of a preferred channel.

A higher value means a better weighting.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

2.111.88.5 Outbound-Server

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].-:%`

2.111.88.6 SSL

This menu contains the parameters for the TLS authentication.

Console path:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.6.1 Versions

This entry specifies which versions of the protocol are allowed.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default:

TLSv1.2

2.111.88.6.2 Keyex-Algorithms

This entry specifies which key-exchange methods are available.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

2.111.88.6.3 Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256
Chacha20-Poly1305

ChaCha20 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*.

Default:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

2.111.88.6.4 Hash-Algorithms

This entry specifies which hash algorithms are allowed and implies which HMAC algorithms are used to protect of the message integrity.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

2.111.88.6.5 Prefer-PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

No
Yes

Default:

Yes

2.111.88.6.6 Renegotiations

With this setting you control whether the client can trigger a renegotiation of SSL/TLS.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

Forbidden
The device disconnects from the remote station if this requests a renegotiation.

Allowed
The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:

Ignored

2.111.88.6.7 Elliptic-Curves

Here you specify which elliptic curves are to be used for encryption.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

secp256r1
secp256r1 is used for encryption.

secp384r1
secp384r1 is used for encryption.

secp521r1
secp521r1 is used for encryption.

ecdh_x25519
ecdh_x25519 is used for encryption.

Default:

secp256r1

secp384r1

secp521r1

ecdh_x25519

2.111.88.6.21 Signature-Hash-Algorithms

Use this entry to specify which hash algorithm is used to encrypt the signature.

Console path:

Setup > **IoT** > **Wireless-ePaper** > **SSL**

Possible values:

MD5-RSA
SHA1-RSA
SHA224-RSA
SHA256-RSA
SHA384-RSA
SHA512-RSA
SHA256-ECDSA
SHA384-ECDSA
SHA512-ECDSA

Default:

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA

2.111.88.7 Loopback-Address

Enter loopback address here.

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.111.90 Bluetooth

This menu allows you to configure Bluetooth devices.

Console path:

Setup > **IoT**

2.111.90.1 iBeacon

This entry allows you to configure the iBeacon module in E-series devices.

Console path:

Setup > **IoT** > **Bluetooth**

2.111.90.1.1 Operating

This entry allows you to set the operating mode of the module.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

No

The module is not enabled.

Manual

iBeacon configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Managed

2.111.90.1.2 UUID

This entry allows you to assign a "universally unique identifier" (UUID) to the iBeacon module.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

Max. 36 characters from `[0-9][a-f][A-F]-`

Default:

00000000-0000-0000-0000-000000000000

2.111.90.1.3 Major

Assign a unique major ID to the iBeacon module.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

2002

2.111.90.1.4 Minor

Assign a unique minor ID to the iBeacon module.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

1001

2.111.90.1.5 Reception-power-shift

Specify the reception power shift.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

Max. 4 characters from `[0-9]-`

-128 … 127

Default:

0

2.111.90.1.6 Transmission-power

Set the transmission power of the iBeacon module.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

Low
The module sends with minimum power.

Medium
The module sends with medium power.

High
The module sends with maximum power.

Default:

High

2.111.90.1.7 Channels

Set which channels the iBeacon module should use to transmit.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

2402MHz
The module transmits on channel 2402.

2426MHz
The module transmits on channel 2426.

2480MHz
The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz
The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

2.111.90.1.8 Coexistence

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

Possible values:

No
Yes

Default:

Yes

2.111.90.1.9 Module-restart

This command causes the iBeacon module to restart.

Console path:

Setup > **IoT** > **Bluetooth** > **iBeacon**

2.111.90.2 Operational

This entry allows you to configure the operating settings for the BLE module in B-series devices.

Console path:

Setup > **IoT** > **Bluetooth**

2.111.90.2.1 Ifc

Select the device BLE interface that is relevant to the settings, e.g. BT-1.

The selection options depend on the equipment of the device.

Console path:

Setup > **IoT** > **Bluetooth** > **Operational**

2.111.90.2.2 Operating

This entry allows you to activate the module.

Console path:

Setup > **IoT** > **Bluetooth** > **Operational**

Possible values:

Yes
The module is enabled.
No
The module is not enabled.

Default:

No

2.111.90.2.3 Operation-Mode

This entry allows you to set the operating mode of the BLE module. Choose whether to use the Bluetooth interface for sending beacons or for scanning the environment.

The two operating modes cannot be operated simultaneously.

Console path:

Setup > **IoT** > **Bluetooth** > **Operational**

Possible values:

BLE-Beacon
The BLE module sends out beacons.

Scanner
The BLE module is used for scanning the environment.

Default:

Scanner

2.111.90.2.4 Scan-Mode

Select here whether to use active or passive scanning. With active scanning, requests are sent actively and any BLE clients in the surroundings can respond to them. This is necessary to determine the names of the clients, for example.

Please note that continuously responding to scan requests can affect client battery life. With passive scanning, no scan requests are sent but only passively listened for.

Console path:

Setup > **IoT** > **Bluetooth** > **Operational**

Possible values:

Passive
Active

Default:

Passive

2.111.90.3 Beacon-Settings

Use this item to configure additional iBeacon parameters on B-series devices.

Console path:

Setup > **IoT** > **Bluetooth**

2.111.90.3.1 Ifc

Select the device BLE interface that is relevant to the settings, e.g. BT-1.

The selection options depend on the equipment of the device.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Settings**

2.111.90.3.2 Beacon-Profiles

Use this item to enter the name of the iBeacon profile created in the Beacon-Profiles table.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Settings**

Possible values:

Max. 17 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.111.90.3.3 Channels

Here you select the BLE channels used to broadcast the iBeacon.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Settings**

Possible values:

2402MHz

The module transmits on channel 2402.

2426MHz

The module transmits on channel 2426.

2480MHz

The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz

The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

2.111.90.3.4 Transmit-Power

Select the transmission power here. The exact meaning of the values that can be selected here is explained in the iBeacon specification.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Settings**

Possible values:

Low
The module sends with minimum power.

Medium
The module sends with medium power.

High
The module sends with maximum power.

Default:

High

2.111.90.4 Beacon-Profiles

Use this item to configure the iBeacon parameters on B-series devices.

Console path:

Setup > **IoT** > **Bluetooth**

2.111.90.4.1 Name

Configure a name for this beacon profile here.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

Default:

empty

2.111.90.4.2 iBeacon-UUID

A 16-byte identifier used to group together larger groups of beacons. For example, all iBeacons of a company could share the same iBeacon UUID.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Profiles**

Possible values:

Max. 36 characters from `[A-Z][a-f][0-9]-`

Default:

empty

2.111.90.4.3 iBeacon-Major

A 2-byte identifier used to distinguish subgroups of iBeacons. For example, all iBeacons at a company branch office could share the same major identifier.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.111.90.4.4 iBeacon-Minor

A 2-byte identifier used to distinguish individual iBeacons. For example, each individual iBeacon in a branch office could have its own minor identifier.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Profiles**

Possible values:

Max. 5 characters from `[0-9]`

Default:

empty

2.111.90.4.5 Measured-Power-Offset

Normally, a power value measured according to the set transmit power is used to detect the approximation and exact distance of devices emitting a beacon. On the basis of the corresponding measurement series, a deviation can be determined between the measured reception power and actual distance from the device emitting the beacon. Based on this deviation, experts can specify a offset of the reference value of the device in order to increase the measurement accuracy.

Console path:

Setup > **IoT** > **Bluetooth** > **Beacon-Profiles**

Possible values:

Max. 16 characters from `[0-9]-`

-128 … 127

Default:

empty

2.112 App-Definitions

Settings for the application definitions for layer-7 detection and layer-7 application control.

Console path:

Setup

2.112.1 Destinations

Table with the destinations for the application definitions for layer-7 detection and layer-7 application control. As soon as the new table contains an entry set for the column *2.112.1.3 Application-Name* on page 1910, the entry is used by layer-7 detection. To be used in the firewall, the name of the entry must explicitly be entered under *2.110.2 DNS-Destination-List* on page 1874.

Console path:

Setup > **App-Definitions**

2.112.1.1 Name

The name for the destination. The name is used to reference this object.

There can be multiple entries for a name by appending the name of the destination with the # character and adding a number with up to three digits (e.g. “LANCOM”, “LANCOM#1”, “LANCOM#2” etc.).

Console path:

Setup > **App-Definitions** > **Destinations**

Possible values:

Max. 32 characters (without #) from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Max. 36 characters (with #) from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.112.1.2 Wildcard-Expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. “*.lancom.*”. The input is limited to 252 characters. If you

need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- UTF-8: Here, one to four bytes must be entered individually as '\x' followed by two hexadecimal digits.
- UTF-16: Here, one or two double bytes must be entered as '\u' followed by four hexadecimal digits.
- UTF-32: Here, the value must be entered as '\U' followed by eight hexadecimal digits.

For the layer-7 application detection, use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

Console path:

Setup > **App-Definitions** > **Destinations**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.112.1.3 Application-Name

Name for the tracking of HTTP/HTTPS connections for layer-7 application detection (e.g. youtube).

Console path:

Setup > **App-Definitions** > **Destinations**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

2.112.1.4 Application-Prio

Set the priority of HTTP/HTTPS tracking by the layer-7 application detection.

Console path:

Setup > **App-Definitions** > **Destinations**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

2.141 VRRP

This menu contains the configuration of VRRP for your IP router.

The Virtual Router Redundancy Protocol enables multiple physical routers to appear as a single “virtual” router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. Only when the master fails, for example as a result of a power outage or if its Internet connection is dropped, will the other routers become active. They will then negotiate with the VRRP protocol to determine which router should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

VRRP operates independently for IPv4 and IPv6, even if configured together in a single line. This is even recommended to ensure that the advertisement interval and priorities are consistent.

Console path:

Setup

2.141.1 Operating

Switch the VRRP module on and off.

Console path:

Setup > **VRRP**

Possible values:

Yes
No

Default:

No

2.141.2 Virtual-Routers

In the Virtual Routers table, the virtual routers can be defined for each interface.

Console path:

Setup > **VRRP**

2.141.2.1 Interface

Logical IPv4 or IPv6 interface or network on which VRRP should be enabled. Only LAN interfaces are supported.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.141.2.2 Router-ID

Unique ID for the virtual router. The router ID is used to consolidate several physical routers into a single virtual router or a standby group. The router ID is sometimes called VRRP ID or VRID for short.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

1 … 255

Default:

1

2.141.2.3 Enabled

Enables or disables VRRP on the interface.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Yes
No

Default:

Yes

2.141.2.4 Version

Defines which VRRP version should be used. Supported are VRRPv2, VRRPv3, or VRRPv2 and VRRPv3. IPv6 is only supported with VRRPv3. IPv4 is supported in both VRRPv2 and VRRPv3.

The v2+v3 mode is intended as a transitional solution for the move from VRRPv2 to VRRPv3 operation under IPv4. It doubles the packet volume, since a virtual router configured in this way sends advertisements in both protocol versions.

A virtual router configured to use one protocol version will discard advertisements from other routers if they have the wrong protocol version, it will be output to the VRRP packet trace and add an entry to the event log table.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

v2
v3
v2+v3

Default:

v3

2.141.2.5 Prio

Specifies the priority with which the virtual router operates. This is transmitted in the advertisements and largely determines which device is the master for a VRRP network. The specified priority must be greater than 0. The value 255 has a special meaning:

- The value 255 is automatically set if the virtual router's address is the same as the address of the interface to which the router is bound. In all other cases, the priority is automatically lowered.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

2.141.2.6 Backup-Prio

The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and cellular support to the cellular interface. Values between 0 and the configured priority are permitted. The value 0 has a special meaning:

- 0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

2.141.2.7 Advert.-Interval

The advertisement interval specifies the time until a virtual router is propagated again. The default value is 100 centiseconds (1 second).

Additionally, version v2 or v2+v3 require the interval to be an integer of 100, since for VRRPv2 the interval must be an integer number of seconds. If the version is subsequently changed, the advert interval is automatically adjusted to a valid value and should be checked.

With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 5 characters from `[0-9]`

Default:

100

2.141.2.8 Virtual-IPv4

Defines the virtual IPv4 address of the virtual router. The address must be identical on all routers in the VRRP network.

To avoid conflicts, virtual IP addresses should only be IP addresses that are not dynamically assigned to end devices that do not speak VRRP.

If the assigned virtual IPv4 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

An unspecified IPv4 address (0.0.0.0) disables IPv4 for this configuration entry.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 15 characters from `[0-9].`

2.141.2.9 Link-Local-Virtual-IPv6

Defines the virtual link-local IPv6 address of the virtual router, for example fe80::1. The address must be identical on all routers in the VRRP network. This address is used as the sender address for sending router advertisements. The parameter is only supported in VRRPv3 mode.

Assigning a virtual link-local address is mandatory to define a virtual router for IPv6.

If the assigned link-local virtual IPv6 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

An unspecified IPv6 address (::) disables IPv6 for this configuration entry.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.141.2.10 Global-Virtual-IPv6

Defines the optional global IPv6 address of the virtual router, for example 2001:db8::1. The address must be identical on all routers in the VRRP network. The parameter is only supported in VRRPv3 mode.

This address is required for the VPN load balancer if it is to operate with IPv6.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

2.141.2.11 Monitored-WAN

Name of the remote site that controls the virtual router behavior. The remote site can still also be assigned to other virtual routers.

Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.141.2.12 Comment

Enter a comment for this entry.

Console path:

Setup > **VRRP** > **Virtual-Routers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.141.3 Master-Holddown-Time

If a time is configured here, the virtual router changes to the "Hold-Down" state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the "Hold-Down" state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the "Master-Holddown-Time" expires, the virtual router transitions to the "Standby" state, in which the monitored WAN connection can be reestablished.

The "Master-Holddown-Time" is a string with a maximum of 6 characters, which may include the digits 0-9 and a colon. This allows the entry of times of up to 999 minutes 59 seconds (999:59).

If there is no colon (e.g. "30") then the specification is interpreted as minutes. In this case the maximum is "999".

If a colon is present, the colon must be followed by two characters that are interpreted as seconds. The maximum possible value here is "59".

Correct time specifications are, for example "5" (5 minutes), "5:30" (5 minutes, 30 seconds) or "0:30" (30 seconds).

A value of "0" or "0:00" disables the Master-Holddown.

Console path:

Setup > **VRRP**

Possible values:

Max. 6 characters from `[0-9]:`

Default:

0:00

2.141.4 Reconnect-Delay

The router will no longer be propagated if the backup connection could not be established. The reconnect delay specifies after how many minutes such a router should in this case attempt to establish its main or backup connection. While the attempt is being made, the router will not be propagated. Input is entered as <minutes>:<seconds>.

Console path:

Setup > **VRRP**

Possible values:

Max. 6 characters from `[0-9]:`

Default:

30:00

2.141.5 Assign-Internal-Services

This item controls whether the virtual router is assigned as a DNS server in DHCPv4, DHCPv6 and Router Advertisement.

Console path:

Setup > VRRP

Possible values:

Yes
No

Default:

Yes

2.141.6 Lan-Link-Detection

Specifies whether the WAN connection should be established if no LAN connection is available.

The feature is relevant for a scenario where the router is still in operation without a LAN connection, but management of the router should be possible via the WAN connection. In this scenario, the LAN-link detection has to be deactivated.

Console path:

Setup > VRRP

Possible values:

Yes
No

Default:

Yes

2.141.7 WAN-Connection-Control

Defines whether VRRP should suppress the connection establishment of the monitored WAN remote peer in standby mode.

Console path:

Setup > VRRP

Possible values:

Disabled

In standby mode, the connection establishment of the monitored WAN remote peer is not suppressed, and the WAN connection is established. Additionally, in this case, the routes to the monitored WAN are not switched when the virtual router switches to standby.

Packets sent to the physical MAC address of the router are not forwarded to the master in standby mode.

Enabled

In standby mode, the connection establishment of the monitored WAN remote peer is suppressed.

Default:

Enabled

2.141.8 V2-Checksum-for-IPv4

Defines how the checksum of VRRPv3 packets for IPv4 should be calculated. For compatibility reasons with third-party network devices, the checksum for VRRPv3 IPv4 can be calculated as in VRRPv2.

Console path:

Setup > **VRRP**

Possible values:

Yes

Calculate the checksum for VRRPv3 IPv4 as in VRRPv2.

No

Do not calculate the checksum for VRRPv3 IPv4 as in VRRPv2.

Default:

No

2.200 Sip-Alg

Configure the settings for the SIP ALG here.

Console path:

Setup

2.200.1 Operating

This setting determines whether the SIP ALG is enabled.

Console path:

Setup > **Sip-Alg**

Possible values:

Yes
No

Default:

No

2.200.2 Firewall-Overrule

This parameter determines whether the firewall applies reject rules to SIP packets or whether the packets are always forwarded by the SIP-ALG.

Console path:

Setup > **Sip-Alg**

Possible values:

No
The firewall applies reject rules to SIP packets.

Yes
The firewall does not apply reject rules to SIP packets. Data packets are always forwarded by the SIP-ALG.

Default:

Yes

2.201 Cloud-Provider

Configuration for special features of the vRouter if it is operated via a cloud provider such as Amazon AWS.

Console path:

Setup

2.201.1 AWS

Entries on the vRouter for the cloud provider Amazon AWS.

Console path:

Setup > **Cloud-Provider**

2.201.1.1 Switch-Route

`do /Setup/Cloud-Provider/AWS/Switch-Route <Profile-Name>`

This command uses the AWS API to switch the prefix in the AWS routing table to the new next hop as configured under *2.201.1.2.1 Profile name* on page 1920.

Console path:

Setup > **Cloud-Provider** > **AWS**

Possible arguments:

<Profile-Name>

Profile name from *2.201.1.2.1 Profile name* on page 1920.

2.201.1.2 HA-Redundancy

Table for the support of vRouter redundancy in AWS.

Console path:

Setup > **Cloud-Provider** > **AWS**

2.201.1.2.1 Profile name

Unique name of the profile. This name is used by the route-change command to reference the profile.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.201.1.2.2 Route-Table

Name of the routing table to change in AWS, e.g. "rtb-099605ce6cb4ac319". This value can be taken from the AWS management interface.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.201.1.2.3 CIDR-IP

Prefix in the routing table for which the next hop is to be changed, e.g. “0.0.0.0/0”.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 18 characters from `[0-9]./`

Default:

empty

2.201.1.2.4 ENI

Name of the AWS network adapter (Elastic Network Interface) that the command is to set as the next hop, e.g. “eni-00c734d6da1fd8968”. This value can be taken from the AWS management interface.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 50 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.201.1.2.5 Region

Region where the AWS route table is located, e.g. “eu-central-1”

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 30 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

2.201.1.2.6 Network name

Name of the interface or remote site used by the vRouter to reach the AWS API, e.g. “INTERNET”.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.201.1.2.7 Comment

Enter a descriptive comment for this entry.

Console path:

Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.201.1.3 Get-Remote-Route-Table

`do /Setup/Cloud-Provider/AWS/Get-Remote-Route-Table <route-table-id> <region> <outgoing-network>`

This command returns the current status of the AWS routing table <route-table-id> via the AWS API. Example:

`do Get-Remote-Route-Table rtb-099605ce6cb4ac319 eu-central-1 INTERNET`

Console path:

Setup > **Cloud-Provider** > **AWS**

Possible arguments:

<route-table-id>

ID of an AWS route table.

<region>

<outgoing-network>

3 Firmware

This menu contains the actions and settings options for managing the device firmware.

Console path:

Firmware

3.1 Version table

This table contains information about the firmware version and serial number of the device.

Console path:

Firmware

3.1.1 Ifc

The interface referred to by the entry.

Console path:

Firmware > **Version-Table**

3.1.2 Module

Full description of the device type.

Console path:

Firmware > **Version-Table**

3.1.3 Version

The firmware version currently active in the device, along with the release date.

Console path:

Firmware > **Version-Table**

3.1.4 Serial number

The device serial number.

Console path:

Firmware > **Version-Table**

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), the status (active or inactive), the firmware version number, the date, the size, and the index (sequential number).

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.

<loader>

This entry is not a firmware version but a loader with offering supporting functions.

3.2.3 Version

Version descriptor of the firmware for the current entry.

Console path:

Firmware > **Table-Firmsafe**

3.2.4 Date

Release date of the firmware for the current entry.

Console path:

Firmware > **Table-Firmsafe**

3.2.5 Size

Size of the firmware for the current entry.

Console path:

Firmware > **Table-Firmsafe**

3.2.6 Index

Index for the current entry.

Console path:

Firmware > **Table-Firmsafe**

3.3 Mode firmsafe

Only one of the two firmware versions stored in the device can be active at any time. When new firmware is uploaded, the currently inactive firmware version will be overwritten. The firmware mode lets you decide which firmware is to be activated after the upload.

It is only possible to upload a second firmware if the device has sufficient memory available for two complete firmware versions. Up-to-date firmware versions (with additional software options, if applicable) may take up more than half of the available memory in older hardware models. In this case these device uses the asymmetric Firmsafe.

Console path:

Firmware

Possible values:

Immediate

This option allows you to upload the new firmware and activate it immediately. The following situations can arise:

The new firmware is uploaded successfully and it then becomes active as desired. Everything is OK.

After uploading the firmware the device no longer responds. If an error occurred during the upload, the device will automatically activate the previous firmware and will restart.

Login

To respond to the problems of a faulty upload, there is a second option to upload and immediately activate the firmware.

In contrast to the first variant, the device then waits for firmsafe timeout while waiting for a successful login via telnet, a terminal program or WEBconfig. Only after this login is the firmware activated.

If the device stops responding or it is not possible to login, then the old firmware is activated automatically and the device starts again.

Manual

The third option allows you set a time period in which you can test the new firmware. The device starts with the new firmware and waits for the set time period for the uploaded firmware to be activated manually, in which case it will be activated permanently. Under LANconfig you activate the new firmware with Device > Firmware management > Release tested firmware, under telnet under **Firmware** > **Firmsafe-Table** with the command "`set # active`", where # is the position of the firmware in the firmsafe table.

Default:

Immediate

3.4 Timeout-Firmsafe

The time in seconds for testing new firmware.

Console path:

Firmware

Possible values:

0 … 99999 Seconds

Default:

300

3.5 Secure upload

When uploading a firmware file, the device checks the integrity of the UPX file by means of a signature in its header (Secure Upload).

Use this directory to configure the Secure Upload.

Console path:

Firmware

3.5.4 LTK hash

This entry contains the hash value of the long-term key.

Console path:

Firmware > **Secure-Upload**

3.7 Feature-Word

Displays the feature bits that provide information on the options activated in the device.

Console path:

Firmware

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

4 Other

This menu contains additional functions from the LCOS menu tree.

Console path:

Other

4.1 Manual dialing

This menu contains the actions for manual connection establishment.

Console path:

Other

4.1.1 Establish

This action prompts a connection to be established to a remote site.

For the action parameter you can enter the name of the corresponding remote site.

Console path:

Other > **Manual-Dialing**

4.1.2 Disconnect

This action causes a connection to a remote site to be disconnected.

For the action parameter you can enter the name of the corresponding remote site.

Console path:

Other > **Manual-Dialing**

4.2 boot-system

With this action you manually restart the device. Parameters can be used to do this at a later time, or or even to delete a planned restart again.

This feature can be used for scenarios where critical changes are made to the configuration, where a misconfiguration could lead to the device being unreachable (e.g. WAN connection or management connection). The command can be

used in conjunction with the test mode “flash no” in which configuration changes are not stored persistently in flash. Example:

1. On the CLI, “flash no” is executed.
2. Set a timed reboot in 30 minutes, e.g. do /other/boot-system 30m
3. Implementing critical configuration changes.
4. › If the changes were successful, the reboot timer can be stopped with “do /other/boot-system stop” and the system can be returned to “flash yes”.
   › If the changes make the device unreachable, the device will automatically reboot after 30 minutes with the old configuration that was active before “flash no” was set.

Console path:

Other

Possible arguments:

<num>s

Restart after a specified duration in seconds, example: do /other/boot-system 10s

<num>m

Restart after a specified time in minutes, example: do /other/boot-system 10m

<num>h

Restart after a specified duration in hours, example: do /other/boot-system 10h

stop

Stop timer, example: do /other/boot-system stop

4.5 Cold-Boot

This action is used to reboot the device. Parameters can be used to execute a cold-boot at a later time, or or even to delete a planned restart again.

This feature can be used for scenarios where critical changes are made to the configuration, where a misconfiguration could lead to the device being unreachable (e.g. WAN connection or management connection). The command can be used in conjunction with the test mode “flash no” in which configuration changes are not stored persistently in flash. Example:

1. On the CLI, “flash no” is executed.
2. Set a timed cold-boot in 30 minutes, e.g. do /other/cold-boot 30m
3. Implementing critical configuration changes.
4. › If the changes were successful, the reboot timer can be stopped with “do /other/cold-boot stop” and the system can be returned to “flash yes”.
   › If the changes make the device unreachable, the device will automatically reboot after 30 minutes with the old configuration that was active before “flash no” was set.

Console path:

Other

Possible arguments:

<num>s

Restart after a specified duration in seconds, example: do /other/cold-boot 10s

<num>m

Restart after a specified time in minutes, example: do /other/cold-boot 10m

<num>h

Restart after a specified duration in hours, example: do /other/cold-boot 10h

stop

Stop timer, example: do /other/cold-boot stop

4.6 Call-Manager

This menu contains the actions for the Call Manager.

Telnet path: /Other/Call-Manager

4.6.1 Line

This menu contains the actions for the Call Manager's lines.

Telnet path: /Other/Call-Manager/Lines

4.6.1.1 Unregister

This action allows you to select a line used by the Call Manager that is to be unregistered.

For the action parameter you can enter the name of the corresponding line.

Telnet path: /Other/Call-Manager/Lines/Unregister

4.6.1.2 Register

This action allows you to select a line used by the Call Manager that is to be registered.

For the action parameter you can enter the name of the corresponding line.

Telnet path: /Other/Call-Manager/Lines/Register

4.6.2 Groups

This menu contains the actions for the Call Manager's groups.

Telnet path: /Other/Call-Manager/Groups

4.6.2.1 show

This action allows you to display a group used by the Call Manager.

For the action parameter you can enter the name of the corresponding group.

Telnet path: /Other/Call-Manager/Groups/Show

4.7 Flash restore

With the device in test mode, you can restore the configuration from the Flash memory. You do this from the command-line interface with the command `do/Other/Flash-Restore`. This command restores the original configuration that was active before executing the command "Flash No" from the Flash memory.

Console path:

Other > **Flash-Restore**

4.8 Enable-Tests

This parameter gives you the option to perform self-tests on the device. You do this from the command-line interface with the command `do/Other/Enable-Tests`.

Please note that once this command is executed, the device exits its normal operating mode. Stability and hardware functioning may be affected.

Console path:

Other > **Enable-Tests**

Appendix

CRON syntax

A CRON job consists of six fields:

```
minute    hour    day of month    month    day of week    command
```

The asterisk '*' serves as a placeholder for all permitted characters.

Here are some examples of performing regular restarts with the use of CRON:

Every day at 13:30h:

```
30          13          *           *           *          restart
```

Every day 30 minutes past each hour:

```
30          *           *           *           *          restart
```

Every 30 minutes every day:

```
*/30        *           *           *           *          restart
```

Every Saturday at 20:15h:

```
15          20          *           *           6          restart
```

Sundays is selected either with '0' or '7'.

At 00:00h on the first day of the month

```
0           0           1           *           *          restart
```