HIRSCHMANN
A BELDEN BRAND

# Reference Manual

## Command Line Interface (CLI)
## HiLCOS Rel. 10.34

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.



The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at:
https://www.doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

# Contents

# Copyright of Integrated Software

**Open Source Software used in the product**

The product contains, among other things, Open Source Software files, as defined below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions.
Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other Hirschmann Automation and Control GmbH license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). Open Source Software contained in this product and the respective Open Source Software licenses are stated below.

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available and such source code is not already delivered together with the product, you can order the corresponding source code of the Open Source Software from Hirschmann Automation and Control GmbH - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the product. Please send your specific request, within three years of the purchase date of this product, together with the name and ID number of the product to be found at the label of the product to:

Hirschmann Automation and Control GmbH
Head of R&D
Stuttgarter Strasse 45-51
72654 Neckartenzlingen
Germany

**Warranty regarding further use of the Open Source Software**

Hirschmann Automation and Control GmbH provides no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Hirschmann Automation and Control GmbH. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Hirschmann Automation and Control GmbH specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Hirschmann Automation and Control GmbH in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:

"This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details."
For the remaining open source components, the liability exclusions of the rights holders in the respective license texts apply.
Technical support, if any, will only be provided for unmodified software.

**Software contained in the product**

You can find the software components which are part of the product and the applicable license terms in the licenses_HiLCOS_10_34.txt file respectively license folder that is included in the HiLCOS 10.34 software bundle.

# 1 Introduction

## 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.

**Note:** 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

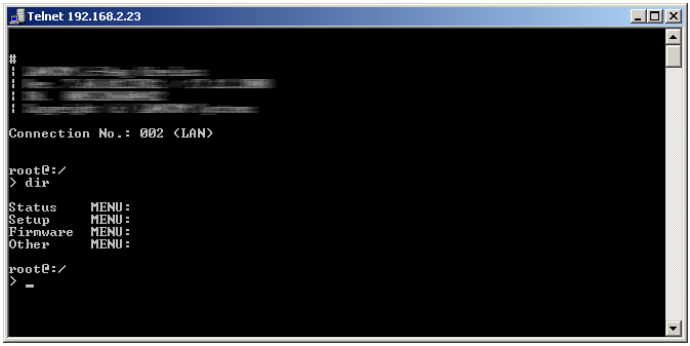
### Close the Telnet session

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

- `C:\>exit`

### Structure of the command-line interface

The command-line interface is always structured as follows:




- **Status**

  Contains the status and statistics of all internal modules in the device

- **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 console

The HiLCOS command-line interface is operated with the following DOS- or UNIX-style commands. Some of the available menu commands can be displayed using the HELP command.

**Note:** Which commands are available depends upon the equipment of the device.

**Important:** 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.

| *Command* | *Description* |
|---|---|
| `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).<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write |
| `readmib` | Display of the SNMP Management Information Base. Available only on devices without a unified MIB.<br>**Access rights**: Supervisor-Read,Local-Admin-Read |
| `readstatus` | Outputs the status of all SNMP IDs for the device. |
| `writeflash` | Load a new firmware file (only via TFTP).<br>**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:<br>▶ `-a`: Specifies the source address of the file:<br>– `a.b.c.d`: Source IP address<br>– `INT`: Use the address of the first intranet interface as the source address<br>– `DMZ`: Use the address of the first DMZ interface as the source address<br>– `LBx`: Use the loopback address x (0..f) as the source address<br>– `<Interface>`: Use the address of the LAN interface <interface> as the source address<br>▶ `-s`: Address of the TFTP server<br>▶ `-n`: Ignore server name on SSL/TLS connections<br>▶ `-f`: <File name> of the configuration file on the TFTP server<br>▶ `-o`: Destination file <file name>for file download<br>▶ `-c`: File <file name> with the root certificate for HTTPS<br>▶ `-p`: File <file name> with unencrypted PKCS#12 container for HTTPS CA certificates and/or client-side authentication<br>▶ `-d`: <Passphrase> to decrypt downloaded encrypted PKCS#12 containers |

| *Command* | *Description* |
|---|---|
| | ▶ `-C`: Checks whether firmware is newer than (n) or different from (d) the current firmware<br>▶ `-m`: Set a minimum <version> of the firmware<br>▶ `-u`: Download firmware file unconditionally; skip the version check.<br>▶ `-x`: File <file name> with additional CA certificates for HTTPS checks; the value ' none' prevents the default certificates from being downloaded<br>▶ `-i`: Send Sysinfo as a POST request (for HTTP(S) only)<br><br>**Note:** 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.<br><br>**Access rights**: Supervisor-Write |
| `language` | Selects a language for the CLI display. The command `language ?` lists the available languages. |
| `ssh [-?\|h] [-<a\|b> Loopback-Address] [-p Port] [-C] [-j Keepalive-Interval] <Host>` | Establishes an SSH connection to the <Host>. Possible arguments are:<br>▶ `-?\|h`: Outputs the help text.<br>▶ `-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 HiLCOS use `-a` to specify a loopback address.<br>▶ `-p`: Sets the <Port> of the host<br>▶ `-C`: Enforces compressed data transfer<br>▶ `-j`: Specifies how frequently the client sends a keepalive. |
| `telnet <Address>` | Establishes a Telnet connection to the given <address>. |
| `sshkeygen [-h] [-q] [-t dsa\|rsa\|ecdsa] [-b <bits>] [-f <file-name>] [-R <host-name>]` | Creates or deletes the SSH key in the device. Possible arguments are:<br>▶ `-h`: Displays a brief help text about the available parameters<br>▶ `-q`: The device overrides existing keys without a prompt (quiet mode)<br>▶ `-t`: This parameter specifies what type of key is generated. SSH supports the following types of keys:<br>– RSA<br>– DSA<br>– ECDSA<br>▶ `-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. |

| *Command* | *Description* |
|---|---|
| | ▶ `-f`: These parameters specify the mounting point of the generated key file in the device file system. The choice of mounting point depends on the type key you are generating. The choices available to you are:<br>– **ssh_rsakey** for RSA keys<br>– **ssh_dsakey** for DSA keys<br>– **ssh_ecdsakey** for ECDSA keys |
| `sshcopyid` | To store your SSH public key using SSH<br>**Access rights**: Supervisor-Write |
| `enable <Parameter>` | Extends the rights of authenticated TACACS+ users. Possible parameters are:<br>▶ `0`: No rights<br>▶ `1`: Read-only<br>▶ `3`: Read-write<br>▶ `5`: Read-only-limited Admin<br>▶ `7`: Read-write-limited Admin<br>▶ `9`: Read-only Admin<br>▶ `11`: Read-write Admin<br>▶ `15`: Supervisor (root) |
| `bootconfig [-s (1\|2\|all)] [-r (1\|2\|all)]` | Enables you to save and delete boot configurations. Options:<br>▶ `-s`: Stores the current configuration of a device either as a custom default setting (1), rollout configuration (2), or both (all).<br>▶ `-r`: Optionally deletes the current custom default setting (1), the rollout configuration (2), or both (all).<br>**Access rights**: Supervisor-Write |
| `lspci` | Output of information via PCI devices<br>**Access rights**: Supervisor-Read |
| `beginscript [-u] [-C d]` | Resets the console 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:<br>▶ `-u`: Forces the **u**nconditional execution of a script or a configuration.<br>▶ `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used.<br>**Access rights**: Supervisor-Write |
| `unmount [-?][-f] <Volume>` | Outputs the current volume table.<br>▶ `-f`: Releases the specified volume. <Volume> may be the volume ID or any mount point.<br>▶ `-?`: Outputs the help text. |

| *Command* | *Description* |
|---|---|
| `cd <Path>` | Switch to the current directory. Various abbreviations can be used, such as replacing `cd ../..` with `cd ...`, etc. |
| `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.<br><br>**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>`.<br><br>The wildcard symbol `*` deletes a table, for example, `del Config/Cron-Table *`.<br><br>**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:<br>▶ `-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.<br>▶ `-r`: Also lists all subdirectories as well as the tables they contain.<br>▶ `-s`: Sorts the display of the current directory; grouped by sub directories, tables, values, and actions; in ascending alphabetical order. |
| `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. |
| `echo <Argument>` | Displays the commands on the console. |
| `exit\|quit\|x` | Ends the terminal session. |
| `feature <Code>` | Activates the software option with the specified activation code.<br><br>**Access rights**: Supervisor-Write |
| `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).<br><br>**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. |
| `iperf [-s\|-c <Host>] [-u] [-p <Port>] [-B <Interface>] [-c] [-b [<Bandw>/]<Bandw>[kKmM]] [-l <Length>] [-t <Time>] [-d] [-r] [-L <Port>] [-h]` | Starts iPerf on the device in order to perform a bandwidth measurement with an iPerf2 remote station. Possible arguments are:<br>▶ **Client/server**<br>– `-u, --udp`: Uses UDP instead of TCP.<br>– `-p, --port <Port>`: Connects with or expects data packets on this port (default: 5001).<br>– `-B, --bind <Interface>`: Permits the connection only via the specified interface (IP address or interface name).<br>▶ **Server specific**<br>– `-s, --server`: Starts iPerf in server mode and waits for an iPerf client to contact it.<br>▶ **Client specific**<br>– `-c, --client <Host>`: Starts iPerf in client mode and connects with the iPerf server <Host> (IP address or DNS name).<br>– `-b, --bandwidth [<Bandw>/]<Bandw>{kKmM}`: Limit the [down]/up-stream bandwidth when analyzing a UDP connection. This Is specified as kilobytes (kK) or megabytes (mM) per second (default: 1 Mbps).<br>– `-l, --len <Length>`: Sets the length of the UDP data packets.<br>– `-t, --time <Time>`: Sets the duration of the connection in seconds (default: 10 seconds).<br>– `-d, --dualtest`: The test is bidirectional: the iPerf server and client send and receive at the same time.<br>– `-r, --tradeoff`: The test is sequential: the iPerf server and client send and receive one after the other.<br>– `-L, --listenport <Port>`: Specifies the port where the device in bidirectional mode expects to receive data packets from the remote iPerf server (default: 5001).<br>▶ **Miscellaneous**<br>– `-h, --help`: Outputs the help text. |
| `killscript <Name>` | Deletes the remaining unprocessed content of a script session Select the script session using its name.<br>**Access rights**: Supervisor-Write |
| `linktest` | Only available on WLAN devices. It displays the results of the WLAN link test.<br>**Access rights**: Supervisor-Write |

| *Command* | *Description* |
|---|---|
| | **Execution right**: WLAN link test |
| `ll2mdetect` | Searches for devices via LL2M in the LAN.<br>**Access rights**: Supervisor-Write |
| `ll2mexec` | Sends one command per LL2M to a device in the LAN.<br>**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.<br>**Access rights**: Supervisor-Write |
| `loadfirmware (-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.<br>**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.<br>**Access rights**: Supervisor-Write |
| `setpass\|passwd [-n <new> <old>]` | Changes the password of the current user account. In order to change the password without having to change the subsequent input request, use the option switch `-n` with the new and old password. |
| `setpass\|passwd [-u <User>][-n <new> <old>]` | Changes the password of the current user account.<br>In order to change the password without a subsequent input prompt, use the option switch `-n` while entering the new and old password.<br>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. |
| `ping <IPv4 address\|hostname>`<br>`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 37. |
| `printenv` | Shows an overview of all environmental variables and their values. |
| `readconfig` | Shows the complete configuration in the format of the device syntax.<br>**Access rights**: Supervisor-Read |
| `readconfig [-h] [-s <password>]` | Shows the complete configuration in the format of the device syntax.<br>▶ `-h`: Adds a checksum to the configuration file.<br>▶ `-s <password>`: Encrypts the configuration file with the use of the specified password. |

| *Command* | *Description* |
|---|---|
| | **Access rights**: Supervisor-Read |
| `readscript [-n] [-d] [-i] [-c] [-m]` | 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:<br>▶ `-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.<br>▶ `-d`: The default values are included in the text output.<br>▶ `-i`: The table designations are included in the text output.<br>▶ `-c`: Includes any comments contained in the script file.<br>▶ `-m`: The text is output to the screen in a compact but difficult to read format (no indentations).<br>**Access rights**: Supervisor-Read |
| `readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>]` | 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:<br>▶ `-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.<br>▶ `-d`: The default values are included in the text output.<br>▶ `-i`: The table designations are included in the text output.<br>▶ `-c`: Includes any comments contained in the script file.<br>▶ `-m`: The text is output to the screen in a compact but difficult to read format (no indentations).<br>▶ `-h`: Adds a checksum to the script file.<br>▶ `-s <password>`: Encrypts the script file with the use of the specified password.<br>**Access rights**: Supervisor-Read |
| `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.<br>The option switch `-x` suppresses the confirmation message.<br>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>` | Release IPv6 address: 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:<br>▶ `wizard`: Deletes the wizard<br>▶ `template`: Deletes the template |

| *Command* | *Description* |
|---|---|
| | ▶ `logo`: Deletes the logo<br>▶ `all`: Deletes the wizard, the template and the logo<br>**Access rights**: Supervisor-Write |
| `sleep [-u] <Value><Suffix>` | Delays the processing of configuration commands by a particular time or terminates them at a particular time.<br>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) or in format `TT.MM.JJJJ hh:mm:ss` (German). Times will only be accepted if the system time has been set. |
| `stop` | Ends the PING command |
| `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.<br>**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.<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write |
| `setenv <Name> <Value>` | Sets an environmental variable to the specified value.<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write |
| `show <Options> <Filter>` | Displays selected internal data, such as the last boot processes (`bootlog`), firewall filter rules (`filter`), VPN rules (`VPN`) or memory utilization (`mem`, `heap`). With additional filter arguments you can further limit the output.<br>For an overview of all possible options, enter `show ?`. For information on displaying IPv6-specific data, read the section *Overview of IPv6-specific show commands* on page 43.<br>**Access rights**: Supervisor-Read,Local-Admin-Read |
| `sysinfo` | Shows the system information (e.g., hardware release, software version, MAC address, serial number, etc.). |
| `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.<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write |

| *Command* | *Description* |
|---|---|
| `time <DateTime>` | Sets a time in format `MM/DD/YYYY hh:mm:ss`.<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write<br>**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 39.<br>**Access rights**: Supervisor-Read,Limited-Admin-Read,Limited-Admin-Write |
| `unsetenv <Name>` | Deletes the specified environmental variable.<br>**Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write |
| `who` | Lists active configuration sessions. |
| `writeconfig [-u] [-C d]` | 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:<br>▶ `-u`: Forces the **u**nconditional execution of a script or a configuration.<br>▶ `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used.<br>**Access rights**: Supervisor-Write |
| `!!` | Repeat last command |
| `!<num>` | Repeat command <num> times |
| `!<prefix>` | Repeat last command beginning with <prefix> |
| `#<blank>` | Comment |

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

### 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.

    **Note:** 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 [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] destination
```

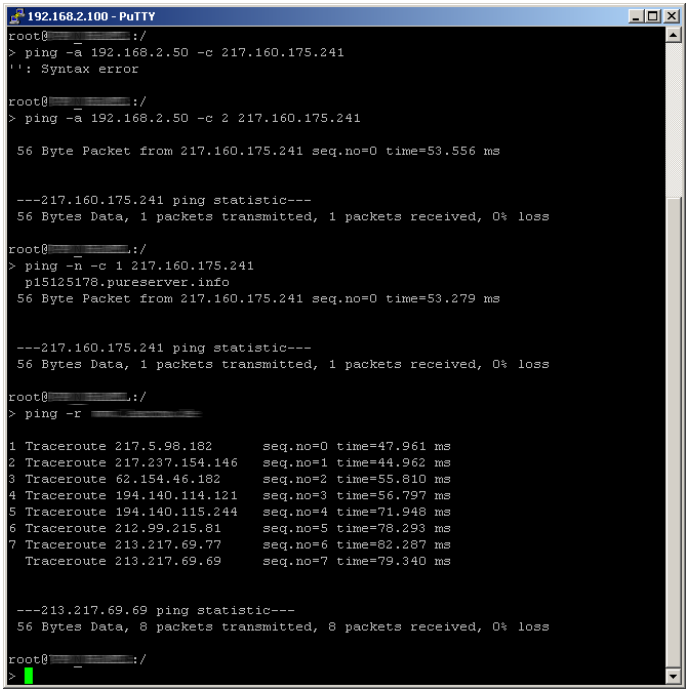
The meaning of the optional parameters is explained in the following table:

| *Parameter* | *Meaning* |
|---|---|
| `-a a.b.c.d` | Sets the ping's sender address (default: IP address of the device. |
| `-a INT` | Sets the intranet address of the device as the sender address |
| `-a DMZ` | Sets the DMZ address of the device as the sender address |
| `-a LBx` | Sets one of the 16 loopback addresses in the device as the sender address. Valid values for x are the hexadecimal values 0 – f |
| `-6 <IPv6-Address>%<Scope>` | Performs a ping command to the link-local address via the interface specified by <scope>.<br>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.<br>**Examples:**<br>▶ `ping -6 fe80::1%INTRANET`<br>Ping the link-local address "fe80::1", which is accessible via the interface and/or the network "INTRANET".<br>▶ `ping -6 2001:db8::1`<br>Pings the global IPv6 address '2001:db8::1". |
| `-6 <Loopback-Interface>` | Sets an IPv6 loopback interface as the sender address. |

| *Parameter* | *Meaning* |
|---|---|
| `-f` | flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example. WARNING: flood ping can easily be misinterpreted as a 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 console (quiet) |
| `-r` | Changes to traceroute mode: The route taken by the data packets underway to the target computer is shown with all of the intermediate stations |
| `-s n` | Sets the packet size to n bytes (max. 65500) |
| `-i n` | Time between packets in seconds |
| `-c n` | Send n ping signals |
| `Destination` | Address or host name of the target computer |

| *Parameter* | *Meaning* |
|---|---|
| `stop /<RETURN>` | Entering "stop" or pressing the RETURN button terminates the ping command |

*Table 2: Overview of optional parameters for the ping command*




## Parameter overview for the trace command

**Note:** The traces available for a particular model can be displayed by entering `trace` without any arguments.

| *This parameter ...* | *...causes the following message in the trace:* |
|---|---|
| `Status` | Connection status messages |
| `Error` | Connection error messages |
| `PPP` | PPP protocol negotiation |

| *This parameter ...* | *...causes the following message in the trace:* |
|---|---|
| `LCR` | Least cost router |
| `Script` | Script negotiation |
| `Firewall` | Displays firewall events |
| `RIP` | IP routing information protocol |
| `ARP` | Address resolution protocol |
| `ICMP` | Internet control message protocol |
| `IP masquerading` | Events in the masquerading module |
| `DHCP` | Dynamic host configuration protocol |
| `NetBIOS` | NetBIOS management |
| `DNS` | Domain name service protocol |
| `Packet dump` | Displays the first 64 bytes of a packet in hexadecimal |
| `ATM cell` | ATM packet layer |
| `ATM error` | ATM error |
| `SMTP client` | E-mail processing by the internal mail client |
| `Mail client` | E-mail processing by the internal mail client |
| `SNTP` | Simple network time protocol |
| `NTP` | Timeserver trace |
| `Connact` | Messages from the activity protocol |
| `Cron` | Activities of the scheduler (cron table) |
| `RADIUS` | RADIUS trace |
| `Serial` | Information on the state of the serial interface |
| `USB` | Information on the state of the USB interface |
| `Load balancer` | Information on load balancing |
| `VRRP` | Information on the virtual router redundancy protocol |
| `Ethernet` | Information on the Ethernet interfaces |
| `VLAN` | Information on virtual networks |
| `IGMP` | Information on the Internet group management protocol |
| `WLAN` | Information on activity in the wireless networks |

| *This parameter ...* | *...causes the following message in the trace:* |
|---|---|
| WLAN-ACL | Status messages about MAC filtering rules.<br><br>**Note:** 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. |
| IAPP | Trace on inter access point protocol giving information on wireless LAN roaming. |
| DFS | Trace on dynamic frequency selection, automatic channel selection in the 5 GHz wireless LAN band |
| Bridge | Information on the wireless LAN bridge |
| EAP | Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1x |
| Spgtree | Information on spanning tree protocol |
| LANAUTH | LAN authentication (e.g. Public Spot) |
| SIP packet | SIP information that is exchanged between a VoIP router and a SIP provider or an upstream SIP telephone system |
| VPN status | IPSec and IKE negotiations |
| VPN packet | IPSec and IKE packets |
| GRE | Messages to GRE tunnels |
| XML-Interface-PbSpot | Messages from the Public Spot XML interface |
| hnat | Information on hardware NAT |
| 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 |
| IPv6 router | Information about the IPv6 routing |
| IPv6-WAN-Packet | Data packets over the IPv6 WAN connection |

*Table 3: Overview of all possible traces*

## Overview of CAPWAP parameters with the show command

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

| *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. |

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

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

| *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. |
| `-a <antenna>` | Shows all APs which have the specified antenna number. |
| `-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. |

| *Parameters* | *Meaning* |
|---|---|
| `-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. |
| `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. |

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

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>)
```

| *Output* | *Comment* |
|---|---|
| Interface | The name of the interface |
| IPv6 address | The IPv6 address |
| Status | The status field can contain the following values:<br>▶ TENTATIVE<br>Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast.<br>▶ PREFERRED<br>The address is valid<br>▶ DEPRECATED<br>The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED.<br>▶ INVALID<br>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: |

| Output | Comment |
|---|---|
| | ▶ None<br>No special attributes<br>▶ (ANYCAST)<br>This is an anycast address<br>▶ (AUTO CONFIG)<br>The address was retrieved by auto-configuration<br>▶ (NO DAD PERFORMED)<br>No DAD is performed |
| Type | The type of IP address |

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

## 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>

| Output | Comment |
|---|---|
| Interface | The name of the interface |

| *Output* | *Comment* |
|---|---|
| Status | The status of the interface Possible entries are:<br>▶ oper status is up<br>▶ oper status is down |
| Forwarding | The forwarding status of the interface. Possible entries are:<br>▶ forwarding is enabled<br>▶ forwarding is disabled |
| Firewall | The status of the firewall. Possible entries are:<br>▶ forwarding is enabled<br>▶ firewall is disabled |

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

## 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>
```

| *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:<br>▶ INCOMPLETE<br>Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined.<br>▶ REACHABLE<br>The neighbor was reached in the last ten seconds.<br>▶ STALE<br>The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. |

| Output | Comment |
|---|---|
| | ▶ DELAY<br>The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols.<br>▶ PROBE<br>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. |

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

## 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].

### Functions for editing commands

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

| Function | 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 HiLCOS menu structure:<br>**1.** If there is only one possibility of completing the command/path, this is accepted by the line.<br>**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.<br>**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. |

## Function keys for the command line

WEBconfig: Setup / Config / 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.

- Key

Name of function key.

Possible values:

– Selection from function keys F1 to F12.

Default:

– F1

▶ Figure

Description of the command/shortcut to be run on calling the function key in the command line.

Possible values:

– All commands/shortcuts possible in the command line

Default:

– Blank

Special values:

– The caret symbol ^ is used to represent 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.

**Note:** 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.

## 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
```

**Note:** 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
```

**Note:** 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
```

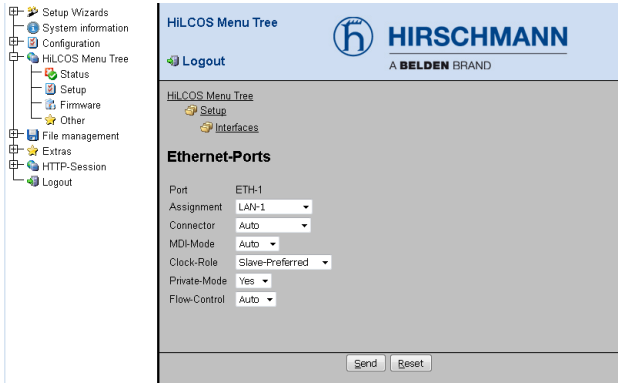
The curly brackets also enable you to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

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

## 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 “HiLCOS Menu Tree” provides the configuration parameters in the same structure as they are used under Telnet.



# 2 Setup

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

**Telnet path:** /Setup

## 2.1 Name

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

**Telnet 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).

**Telnet path:**
**Setup**

### 2.2.2 Dialup-Peers

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

**Note:** 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.

**Telnet path:**

**Setup** > **WAN**

## 2.2.2.1 Remote site

Enter the name of the remote site here.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 9999

**Default:**

0

### 2.2.2.4 B2-DT

Hold time for bundling: When channels are bundled, the second B channel will be terminated if it is not used for the time entered here.

**Telnet 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. For example, you should use the PPPHDLC entry to establish a PPP connection to an Internet provider.

**Telnet path:**

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

**Possible values:**

Select from the list of defined layers

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

**Default:**

*empty*

## 2.2.2.6 Callback

With callback activated, an incoming call from this remote site will not be answered, but it will be called back instead.

This is useful if, for example, telephone fees are to be avoided at the remote site.

Activate a check of the name if you want to be sure that the remote site is authenticated before the callback.

Select the fast option if the callback is to follow within seconds. The remote site must also support this method and the 'Expect callback' option must be activated. Additionally, the remote site must be entered into the number list.

**Note:** The setting 'Name' offers the highest security if there is an entry in the numbers list and in the PPP list. The setting 'Hirschmann' enables the fastest method of call-back between two devices from Hirschmann.

**Note:** For Windows remote sites, ensure that you select the setting 'Name'.

**Telnet path:**

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

**Possible values:**

**No**

There is no return call.

**Auto**

If the remote site is found in the numbers list, this number is called back. Initially the call is rejected and, as soon as the channel is free again, a return call is made (after approx. 8 seconds). If the remote site is not found in the numbers list, the DEFAULT remote site is initially taken and the return call is negotiated during the protocol negotiation. The call is charged with one unit.

**Name**

Before a return call is made, the protocol is always negotiated even if the remote site is found in the numbers list (e.g. for Windows computers that dial-in to the device). Small call charges are incurred for this.

**fast**

If the remote site is found in the numbers list, the return call is made quickly, i.e. the device sends a special signal to the remote site and it calls back as soon as the channel is free again. The connection is established within about 2 seconds. If the remote site does not cancel the call immediately after the signal, then two seconds later it reverts to the normal return call procedure (lasts about 8 seconds). This procedure is available with DSS1 connections only.

**Looser**

Use the "looser" option if a return call from the remote site is expected. This setting fulfills two jobs in one. Firstly it ensures that a connection it established itself terminates if a call arrives from the remote site that was just called, and secondly this setting activates the function that reacts to the procedure for fast return calls. This means that to use fast return calls, the caller must be in 'Looser' mode and, at the called party, the return call must be set to 'Hirschmann'.

**Default:**

No

### 2.2.3 RoundRobin

If a remote site can be reached at various call numbers. you can enter these numbers into this list.

**Telnet path:**

**Setup** > **WAN**

#### 2.2.3.1 Remote site

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

**Telnet path:**

**Setup** > **WAN** > **RoundRobin**

**Possible values:**

Select from the list of defined peers.

Max. 18 characters from
`#[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

### 2.2.3.2 Round-Robin

Specify here the other call numbers for this peer. Separate the individual call numbers with hyphens.

**Telnet path:**

**Setup** > **WAN** > **RoundRobin**

**Possible values:**

Max. 53 characters from `0123456789S*#-EF:`

**Default:**

*empty*

### 2.2.3.3 Head

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

**Telnet path:**

**Setup** > **WAN** > **RoundRobin**

**Possible values:**

**Last**
**First**

**Default:**
Last

### 2.2.4 Layer

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

**Telnet path:**
**Setup** > **WAN**

## 2.2.4.1 Layer name

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

**Telnet 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.

**Telnet 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:

**Telnet 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.

**APPP**
AsyncPPP: Like 'PPP', but here the asynchronous mode is used instead. PPP works with characters.

**SCPPP**
PPP with its own script. The script is specified in the script list.

**SCAPPP**
AsyncPPP with its own script. The script is specified in the script list.

**SCTRANS**
Transparent with its own script. The script is specified in the script list.

**DHCP**
Allocation of network parameters by 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.

**Telnet path:**
**Setup** > **WAN** > **Layer**

**Possible values:**

**PPPoE**
PPP over Ethernet: PPP information is encapsulated in Ethernet frames

**TRANS**
Transparent: No additional header is inserted.

**X.75LABP**
Connections are established with X.75 and LAPM (Link Access Procedure Balanced).

**Default:**
X.75LABP

## 2.2.4.5 L2-Opt.

Here you can activate the compression of transmitted data . These options are only come into effect if they are supported by the interfaces used and by the selected Layer 2 and Layer 3 protocols.

**Telnet path:**

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

**Possible values:**

**None**

**compr.**

Compression

**Default:**

None

## 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.

**Telnet path:**

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

**Possible values:**

**ETH**

Transparent Ethernet as per IEEE 802.3

**SERIAL**

For connections by analog modem or cellular modem with AT interface. The modem can be connected to the device via the serial port (outband).

**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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

**IP**
**IP+NBT**
**IPX**
**IP+IPX**
**IP+NBT+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.

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

**Telnet path:**

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

**Possible values:**

**MS-CHAPv2**
**MS-CHAP**
**CHAP**
**PAP**

**Default:**

MS-CHAPv2
MS-CHAP
CHAP
PAP

### 2.2.6 Incoming calling numbers

Based on the telephone numbers in this list, your device can identify which remote site is making the incoming call.

**Telnet path:**

**Setup** > **WAN**

## 2.2.6.1 Dialup remote

Here you enter the call number that is transmitted when you are called from the remote site. Generally this is the number of the remote site combined with the corresponding local area code with the leading zero, e.g. 0221445566. For remote sites in other countries, you must add the corresponding country code with two leading zeros, e.g. 0049221445566.

**Telnet path:**

**Setup** > **WAN** > **Incoming calling numbers**

**Possible values:**

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

**Default:**

*empty*

### 2.2.6.2 Remote site

Enter the name of the relevant remote site. Once a device has identified a remote site by means of its call number, the list of peers/remote sites is searched for an entry with that name and the associated settings are used for the connection.

**Telnet path:**

**Setup** > **WAN** > **Incoming calling numbers**

**Possible values:**

Select from the list of defined peers.

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

**Default:**

*empty*

## 2.2.8 Scripts

If a login script has to be processed when connecting to a remote site, enter the script here.

**Telnet path:**

**Setup** > **WAN**

### 2.2.8.1 Remote site

Enter the name of the remote site here. The remote site should already have been entered into the list of peers / remote sites. You can also select an entry directly from the list of peers / remote sites.

**Telnet path:**

**Setup** > **WAN** > **Scripts**

**Possible values:**

Select from the list of defined peers.

Max. 18 characters from
`#[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

### 2.2.8.2 Script

Specify here the login script for this peer. In order for this script to be used, a layer with the appropriate protocol for this peer must be set up in the list or peers / remote sites.

**Telnet path:**

**Setup** > **WAN** > **Scripts**

**Possible values:**

Max. 58 characters from
`#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

## 2.2.9 Protect

Here you set the conditions to be satisfied in order for the device to accept incoming calls.

**Telnet path:**

**Setup** > **WAN**

**Possible values:**

**None**

The device answers any call.

**Number**

The device will receive a call only if the caller's number is transmitted and if that number is in the number list.

**Screened**

The machine will only accept a call if the caller is in the number list, the caller's number is transmitted, and if the number has been checked by the exchange.

**Default:**

None

## 2.2.10 Callback attempts

Set the number of callback attempts for automatic callback connections.

**Telnet path:**

**Setup** > **WAN**

**Possible values:**

0 … 9

**Default:**

3

### 2.2.11 Router interface

Enter here further settings for each WAN interface used by the device, for example the calling numbers to be used.

**Telnet path:**

**Setup** > **WAN**

## 2.2.11.1 Ifc

WAN interface to which the settings in this entry apply.

**Telnet path:**

**Setup** > **WAN** > **Router-Interface**

## 2.2.11.2 MSN/EAZ

Specify here for this interface the call numbers for which the device should accept incoming calls. As a rule these numbers are the call numbers of the interface without an area code, or the internal call number behind a PBX, as appropriate. Multiple number can be entered by separating them with a semi-colon. The first call number is used for outgoing calls.

**Note:** If you specify any number outside of your number pool, the device will accept no calls at all.

**Note:** If you do not enter a number here, the device will accept all calls.

**Telnet path:**

**Setup** > **WAN** > **Router-Interface**

**Possible values:**

Max. 30 characters from `#0123456789`

**Default:**
*empty*

## 2.2.11.3 CLIP

Activate this option if a peer called by the device should not see your call number.

**Note:** This function must be supported by your network operator.

**Telnet path:**
**Setup** > **WAN** > **Router-Interface**

**Possible values:**
**Yes**
**No**

**Default:**
Yes

## 2.2.11.8 YC.

Y connection: This setting determines what happens when channel bundling is in operation and a request for a second connection arrives.

**Note:** Please note that channel bundling incurs costs for two connections. No further connections can be made over LANCAPI! Only use channel bundling when the full transfer speed is required and used.

**Telnet path:**

**Setup** > **WAN** > **Router-Interface**

**Possible values:**

**Yes**

The device interrupts channel bundling to establish the second connection to the other remote device. If the second channel becomes free again, it is automatically used for channel bundling again (always for static bundling, when required for dynamic bundling).

**No**

The device maintains the existing bundled connection; the second connection must wait.

**Default:**

Yes

## 2.2.11.9 Accept-calls

Specify here whether the device answers calls to this interface or not.

**Note:** If you have specified a number for device configuration (Management / Admin), all calls with this number will be accepted, whatever you select here.

**Telnet path:**

**Setup** > **WAN** > **Router-Interface**

**Possible values:**

**all**

**None**

**Default:**

all

### 2.2.13 Manual dialing

This menu contains the settings for manual dialing.

**Telnet path:**

**Setup** > **WAN**

## 2.2.13.1 Establish

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

**Telnet 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.

**Telnet path:**

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

**Possible arguments:**

**<Remote>**

Name of a remote site defined in the device.

### 2.2.18 Backup-Delay-Seconds

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

**Telnet 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.

**Telnet path:**

**Setup** > **WAN**

## 2.2.19.1 Remote site

Enter the name of the remote site here.

**Telnet 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 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.

**Telnet path:**
**Setup** > **WAN** > **DSL-Broadband-Peers**

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

**Default:**
*empty*

## 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

## 2.2.19.13 user-def.-MAC

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

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 9999

**Default:**

0

### 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.

**Telnet 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**.

**Telnet path:**

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

**Possible values:**

Select from the list of defined peers.

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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**
**Setup** > **WAN** > **IP-List**

**Possible values:**
Valid IPv4 address, max. 15 characters from `[0-9].`

**Default:**
0.0.0.0

## 2.2.20.7 NBNS-Default

Specify here the address of a NetBIOS name server to which NBNS 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 NetBIOS name server to the device when it logs in.

**Telnet path:**

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

**Possible values:**

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

**Default:**

0.0.0.0

## 2.2.20.8 NBNS-Backup

IP address of the NetBIOS name server for the forwarding of NetBIOS requests. Default: 0.0.0.0 The IP address of the device in this network is communicated as the NBNS server if the NetBIOS proxy is activated for this network. If the NetBIOS proxy is not active for this network, then the IP address in the global TCP/IP settings is communicated as the NBNS server.

**Telnet 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.

**Note:** 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.

**Note:** 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WAN**

### 2.2.21.1 Remote site

This name from the list of DSL broadband peers.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

**Off**
**40-Bits**
**56-Bits**
**128-Bits**

**Default:**

Off

## 2.2.22 RADIUS

This menu contains the settings for the RADIUS server.

**Telnet path:**
**Setup** > **WAN**

## 2.2.22.1 Operating

Switches RADIUS authentication on/off.

**Telnet 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.

**Telnet 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.

**Telnet 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.

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

**Telnet 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

## 2.2.22.6 CLIP operation

When remote sites dial in, the internal call number list, or alternatively an external RADIUS server, can be used for authentication.

**Note:** The dial-in remote sites must be configured in the RADIUS server such that the name of the entry corresponds to the call number of the remote site dialing in.

**Telnet path:**

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

**Possible values:**

**Yes**

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

**No**

No external RADIUS server is used for authentication of dial-in remote sites.

**Exclusive**

Enables the use of an external RADIUS server as the only possibility for authenticating dial-in remote sites. The call number list is ignored.

**Default:**

No

## 2.2.22.7 CLIP password

Password for the log-in of dial-in remote sites to the external RADIUS server.

**Note:** The dial-in remote sites must be configured in the RADIUS server such that all the entries for all call numbers use the password configured here.

**Telnet path:**

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

**Possible values:**

Max. 31 characters from

**Default:**

*empty*

## 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.

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

**Telnet 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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet 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`.

**Telnet 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.

**Telnet 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

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

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 65535

## 2.2.22.23 Loopback-Address

The sender address used for RADIUS requests.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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`.

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

### 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.

**Telnet path:**

**Setup** > **WAN**

## 2.2.23.1 Remote site

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

**Telnet 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.

**Telnet 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.

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

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

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

**Telnet 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.

**Telnet path:**

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

**Possible values:**

**Forced**

The device polls in the given interval. This is the default behavior of HiLCOS 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.

**Telnet path:**

**Setup** > **WAN**

## 2.2.24.1 Remote site

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

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 4294967295

**Default:**

0

### 2.2.25.2 Host name

Action name. This name can be referenced in the fields 'Action' and 'Check for' with the place holder %h (host name).

**Telnet path:**

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

**Possible values:**

Max. 64 characters

**Default:**

*empty*

### 2.2.25.3 Remote site

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

**Telnet 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 Block time

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

**Telnet 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.

**Telnet 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 a DSN name resolution. For example, the action “dnscheck:myserver.dyndns.org” requests the IP 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
- 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 IP 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.

**Telnet 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 IP 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.

**Telnet path:**

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

**Possible values:**
Max. 50 characters

**Default:**
*empty*

## 2.2.25.8 Operating

Activates or deactivates this entry.

**Telnet 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.

**Telnet 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.

**Telnet path:**
**Setup** > **WAN** > **Action-Table**

**Possible values:**
0 … 65535

**Default:**
0

## 2.2.26 MTU-List

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

**Telnet path:**
**Setup** > **WAN**

## 2.2.26.1 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.

**Telnet path:**

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

**Possible values:**

Select 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WAN**

## 2.2.30.1 Remote site

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

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WAN**

**Possible values:**

**Address**

The PPTP checks the address only. This is the standard behavior of older versions of HiLCOS 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.

**Note:** 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.

**Telnet 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.

**Telnet 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).

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 65535

## 2.2.35.4 Port

UDP port to be used.

**Telnet path:**

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

**Possible values:**

0 … 65535

**Default:**

1701

## 2.2.35.5 Poll

The polling interval in seconds.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

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

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

**Telnet 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:**

## 2.2.36 L2TP-Additional-Gateways

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

**Telnet path:**

**Setup** > **WAN**

## 2.2.36.1 Identifier

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

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WAN**

### 2.2.37.1 Remote site

Name of the L2TP remote station.

**Telnet 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

**Telnet 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.

**Telnet path:**

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

**Possible values:**

0 … 9999

## 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.

**Telnet path:**

**Setup** > **WAN**

**Possible values:**

**Address**
**Tag+address**

**Default:**
Address

## 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.

**Telnet path:**
**Setup** > **WAN**

## 2.2.40.1 Name

Enter the name for the tunnel.

**Telnet 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 "::".

**Telnet 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.

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

### 2.2.50 EoGRE-Tunnel

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

**Telnet path:**

**Setup** > **WAN**

## 2.2.50.1 Interface

Name of the selected EoGRE tunnel.

**Telnet 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.

**Telnet 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).

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

**Yes**
**No**

**Default:**

No

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WAN** > **GRE-Tunnel**

## 2.2.51.3 IP address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

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

**Telnet 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:**

## 2.3 Charges

This menu contains the settings for charge management.

**SNMP ID:** 2.3

**Telnet 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.

**SNMP ID:** 2.3.2

**Telnet path:** /Setup/Charges

**Possible values:**

- Max. 10 characters

**Default:** 1

### 2.3.7 Time-Table

This table displays an overview of configured budgets for your interfaces, sorted by budget minutes.

**SNMP ID:** 2.3.7

**Telnet path:** /Setup/Charges

#### 2.3.7.1 Ifc.

The interface referred to by the entry.

**SNMP ID:** 2.3.7.1

**Telnet path:** /Setup/Charges/Time-Table

#### 2.3.7.2 Budget-minutes

Displays the budgeted minutes used up for this interface.

**SNMP ID:** 2.3.7.2

**Telnet path:** /Setup/Charges/Time-Table

#### 2.3.7.3 Spare-Minutes

Displays the remaining budgeted minutes for this interface.

**SNMP ID:** 2.3.7.3

**Telnet path:** /Setup/Charges/Time-Table

### 2.3.7.4 Minutes-active

Displays the budgeted minutes of activity for data connections on this interface.

**SNMP ID:** 2.3.7.4

**Telnet path:** /Setup/Charges/Time-Table

### 2.3.7.5 Minutes-passive

Displays the budgeted minutes that this interface was connected passively.

**SNMP ID:** 2.3.7.5

**Telnet 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.

**SNMP ID:** 2.3.8

**Telnet path:** /Setup/Charges

**Possible values:**

- Max. 10 characters

**Default:** 600

### 2.3.9 Spare-DSL-Broadband-Minutes

Displays the number of minutes remaining for DSL broadband connections in the current period.

**SNMP ID:** 2.3.9

**Telnet 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.

**SNMP ID:** 2.3.10

**Telnet 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.

**SNMP ID:** 2.3.11

**Telnet path:** /Setup/Charges

**Possible values:**

- Max. 10 characters

**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.

**Note:** By resetting the current budget, you remove any charge limiter that may be in effect.

**Telnet path:**

**Setup** > **Charges**

### 2.3.13 Dialup-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.

**SNMP ID:** 2.3.13

**Telnet path:** /Setup/Charges

**Possible values:**

- Max. 10 characters

**Default:** 210

## 2.3.14 Spare-Dialup-Minutes

Displays the number of minutes remaining for dial-in connections in the current period.

**SNMP ID:** 2.3.14

**Telnet path:** /Setup/Charges

## 2.3.15 Dialup-Minutes-Active

Displays the number of minutes used by dial-in connections in the current time period.

**SNMP ID:** 2.3.15

**Telnet path:** /Setup/Charges

## 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.

**Note:** By activating an additional budget, you remove any charge limiter that may be in effect.

### Telnet path:

**Setup** > **Charges**

# 2.4 LAN

This item contains the settings for the LAN.

**SNMP ID:** 2.4

**Telnet path:** /Setup/LAN

## 2.4.2 MAC-Address

This is the hardware address of the network adapter in your device.

**SNMP ID:** 2.4.2

**Telnet path:** /Setup/LAN/MAC-Address

## 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).

**SNMP ID:** 2.4.3

**Telnet path:** /Setup/LAN/Spare-Heap

**Possible values**:

- Max. 3 numeric characters in the range 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.

**SNMP ID:** 2.4.8

**Telnet path:** /Setup/LAN/Trace-MAC

**Possible values**:

- 12 hexadecimal characters

**Default**: 000000000000

**Special values:** 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.

**SNMP ID:** 2.4.9

**Telnet path:** /Setup/LAN/Trace-Level

**Possible values**:

- Numerical characters from 0 to 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.

**SNMP ID:** 2.4.10

**Telnet path:** /Setup/LAN/IEEE802.1x

## 2.4.10.1 Supplicant-Ifc-Setup

This table controls the function of the integrated 802.1x supplicant for the available LAN interfaces.

**SNMP ID:** 2.4.10.1

**Telnet path:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup

### 2.4.10.1.1 Ifc

Here you select the LAN interface that the settings for the 802.1x supplicant apply to.

**SNMP ID:** 2.4.10.1.1

**Telnet path:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Ifc

**Possible values**:

- Choose from the LAN interfaces available in the device, e.g. LAN-1 or LAN-2.

**Default**: LAN-1

### 2.4.10.1.2 Method

Here you select the method to be used by the 802.1x supplicant for authentication.

**SNMP ID:** 2.4.10.1.2

**Telnet path:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Method

**Possible values**:

- None
- MD5
- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5

- PEAP/MSCHAPv2
- PEAP/GTC

**Default**: None

**Special values:** The value "None" disables the 802.1x supplicant for the respective interface.

#### 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'.

**SNMP ID:** 2.4.10.1.3

**Telnet path:** /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Credentials

**Possible values**:

- Max. 64 alphanumerical characters

**Default**: Blank

### 2.4.10.2 Authenticator-Ifc-Setup

This menu contains the settings for the RADIUS authentication of clients, which connect to the device via the LAN interfaces.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x**

#### 2.4.10.2.1 Ifc

Name of the LAN interface.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

### 2.4.10.2.2 Operating

This parameter specifies whether RADIUS authentication of clients is required on the selected LAN interface.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

**Possible values:**

**No**
**Yes**

**Default:**

No

### 2.4.10.2.3 Mode

This item sets whether one or more clients may login at this interface via IEEE 802.1X.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

**Possible values:**

**Single host**
Just one client may login to this interface.

**Multiple host**
Multiple clients may login to this interface. Just one client needs to successfully login to the interface. The device automatically authenticates all other clients at this interface. However, if the connection to the authenticated device is closed, all of the other clients are no longer able to use the connection.

**Multiple auth**
Multiple clients can login to this interface; each client must authenticate itself.

**Default:**

Single host

### 2.4.10.2.4 RADIUS server

This parameter specifies the RADIUS server to be used by the device to authenticate the LAN clients.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

**Possible values:**

**Name** from **Setup** > **IEEE802.1x** > **RADIUS-Server**

Valid IPv4/v6 address or FQDN, max. 16 characters from `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

### 2.4.10.2.5 MAC-Auth.-Bypass

In order for a device that does not support IEEE 802.1X to authenticate at this interface, selecting this option takes the MAC address of the device to be the user name and password.

**Important:** The MAC address is easy to fake and does not protect against malicious attacks.

**Telnet path:**

**Setup** > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

**Possible values:**

**No**

MAC address authentication is not possible.

**Yes**

MAC address authentication is possible.

**Default:**

No

## 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.

**Telnet path:**

**Setup** > **LAN** > **Linkup-Report-Delay-ms**

**Possible values:**

0 to 4294967295

**Default:**

50

## 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.

**Telnet path:**

**Setup** > **LAN**

## 2.4.13.1 Interfaces

This menu contains the settings for interface bundling.

**Telnet 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.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **Interfaces**

**Possible values:**

**PRP-1**
**PRP-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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **Interfaces**

**Possible values:**

Select from the available interfaces.

**Default:**

WLAN-2

## 2.4.13.11 Interfaces

This menu contains the settings for PRP as the bundling protocol.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

### 2.4.13.11.1 Interfaces

This table contains the interfaces with all PRP-relevant settings.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

#### *2.4.13.11.1.1 Interface*

The parallel redundancy protocol (PRP) makes redundant transmissions on two (bundled) interfaces. To use this, you select two interfaces which the device internally combines into one interface. The device duplicates outgoing packets so that the packets are transmitted on each of the two interfaces. On the receiving side, the device recognizes the duplicates and discards them. This leads to a reduced packet error rate and to lower latency on the bundled interface in comparison to transmission on a single interface.

You enter the name for this interface here.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

Max. 18 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

#### *2.4.13.11.1.2 Duplicate-accept*

Switches the forwarding of packet duplicates on or off.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

**Special values:**

**Yes**
**No**

### *2.4.13.11.1.3 Transparent mode*

Switches the transparent operation mode on/off. If the transparent operation mode is enabled, the recipient of the PRP packets forwards the packets with a redundancy control trailer.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

**Yes**
**No**

**Default:**

No

### *2.4.13.11.1.4 Life check interval*

Specifies how often the device sends control packets.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

100 … 60000 Milliseconds

**Default:**

2000

### *2.4.13.11.1.5 Node forget time*

Enters the time until the device deletes a node from its node table or proxy node table.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

1000 … 3600000 Milliseconds

**Default:**

60000

### *2.4.13.11.1.6 Entry forget time*

Specifies as of when the device deletes the entry from the duplicate-detection buffer.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

10 … 60000 Milliseconds

**Default:**

400

### *2.4.13.11.1.7 Node reboot interval*

Specifies the time that a PRP device passively monitors a link until the device sends packets over the link.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

0 … 60000 Milliseconds

**Default:**

500

### *2.4.11.1.8 Dup elimination buffer size*

Limits the number of entries in the duplicate-detection memory.

**Telnet path:**

**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

16 … 65536 Entries/Nodes

**Default:**

8192

### *2.4.13.11.1.9 Send supervision frames*

Specifies the settings for sending supervision packets.

**Telnet path:**

**LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

**0**
None

**1**
Own MAC only

**2**
All-nodes

**Default:**
2

### *2.4.13.11.1.10 Node name*

The node name is the identifier for the node. You can specify any name.

**Telnet path:**
**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

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

### *2.4.13.11.1.11 Evaluate-Sup.-Frames*

Switches the monitoring of control packets on or off.

**Telnet path:**
**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

**Yes**
**No**

**Default:**
Yes

### *2.4.13.11.1.248 Reordering-buffer-on*

Enable or disable the PRP micro-reordering buffer here.

**Telnet path:**
**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

**Possible values:**

**No**
PRP micro-reordering buffer off

**Yes**
PRP micro-reordering buffer on

**Default:**
No

### *2.4.13.11.1.249 Reordering-buffer-max-delay*

Specify the maximum delay time for PRP frames here.

**Telnet path:**
**Setup** > **LAN** > **Interface-bundling** > **PRP** > **Interfaces**

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

**Default:**
50

#### *2.4.13.11.1.250 Force-PRP-transmission*

Here you enable or disable the function to force the transmission to contain the Redundancy Control Trailer (RCT) on both interfaces.

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **PRP** > **Interfaces**

**Possible values:**

**No**

Function to force the transmission to contain the Redundancy Control Trailer (RCT) on both interfaces disabled

**Yes**

Function to force the transmission to contain the Redundancy Control Trailer (RCT) on both interfaces enabled

**Default:**

No

## 2.7 TCP-IP

This menu contains the TCP/IP settings.

**SNMP ID:** 2.7

**Telnet path:** /Setup

### 2.7.1 Operating

Activates or deactivates the TCP-IP module.

**SNMP ID:** 2.7.1

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- Yes

- No

**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.

**SNMP ID:** 2.7.6

**Telnet path:** /Setup/TCP-IP

## 2.7.6.1 IP-Address

IP address of the station that is to be granted access to the device's configuration.

**SNMP ID:** 2.7.6.1

**Telnet path:** /Setup/TCP-IP/Access-List

**Possible values:**

- Valid IP address

## 2.7.6.2 IP-Netmask

IP netmask of the station that is to be given access to the device's configuration.

**SNMP ID:** 2.7.6.2

**Telnet path:** /Setup/TCP-IP/Access-List

**Possible values:**

- Valid IP address

## 2.7.6.3 Rtg-Tag

Routing tag for selecting a specified route.

**SNMP ID:** 2.7.6.3

**Telnet path:** /Setup/TCP-IP/Access-List

**Possible values:** Max. 5 characters

### 2.7.6.4 Comment

This parameter allows you to enter a comment on the entry.

**Telnet 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.

**SNMP ID:** 2.7.7

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.7.8

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.7.9 NBNS-Default

Specify here the address of a NetBIOS name server to which NBNS 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 NetBIOS name server to the device when it logs in.

**SNMP ID:** 2.7.9

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.7.10 NBNS-Backup

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

**SNMP ID:** 2.7.10

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.7.11

**Telnet path:** /Setup/TCP-IP

**Possible values:**

- 1 to 60 minutes

**Default:** 15 minutes

## 2.7.12 TCP-Aging-Minutes

Specify the time in minutes after which the TCP table is updated automatically, i.e. any addresses that have not been contacted since the last update are removed from the list.

**Telnet path:**

**Setup** > **TCP-IP**

**Possible values:**

Max. 2 characters from `[0-6]`

1 … 60

**Default:**

15

## 2.7.13 TCP-Max.-Conn.

This entry places a limit on the maximum number of TCP connections.

**Telnet path:**

**Setup** > **TCP-IP**

**Possible values:**

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

0 … 255

**Special values:**

**0**

This value disables the limitation on the number of TCP connections.

**Default:**

0

## 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.

**SNMP ID:** 2.7.16

**Telnet path:** /Setup/TCP-IP

## 2.7.16.1 IP-Address

IP address for which a MAC address was determined.

**SNMP ID:** 2.7.16.1

**Telnet path:** /Setup/TCP-IP/ARP-Table

**Possible values:**

- Valid IP address

## 2.7.16.2 MAC-Address

MAC address matching the IP address in this entry.

**SNMP ID:** 2.7.16.2

**Telnet path:** /Setup/TCP-IP/ARP-Table

## 2.7.16.3 Last-access

The time when this station last access the network.

**SNMP ID:** 2.7.16.3

**Telnet path:** /Setup/TCP-IP/ARP-Table

## 2.7.16.5 Ethernet-Port

Physical interface connecting the station to the device.

**SNMP ID:** 2.7.16.5

**Telnet path:** /Setup/TCP-IP/ARP-Table

### 2.7.16.6 Peer

Remote device over which the station can be reached.

**SNMP ID:** 2.7.16.6

**Telnet path:** /Setup/TCP-IP/ARP-Table

**Possible values:**

- Select from the list of defined peers.

### 2.7.16.7 VLAN-ID

VLAN ID of network where the station is located.

**SNMP ID:** 2.7.16.7

**Telnet path:** /Setup/TCP-IP/ARP-Table

### 2.7.16.8 Connector

Logical interface connecting the device.

**SNMP ID:** 2.7.16.8

**Telnet path:** /Setup/TCP-IP/ARP-Table/Connect

**Possible values:**

- A parameter from the list of logical interfaces.

## 2.7.17 Loopback-List

This table is used to configure alternative addresses.

**SNMP ID:** 2.7.17

**Telnet path:** /Setup/TCP-IP

## 2.7.17.1 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.

**SNMP ID:** 2.7.17.1

**Telnet path:** /Setup/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

**Default:** 0.0.0.0

## 2.7.17.2 Name

You can enter a name with a max. 16 characters here

**SNMP ID:** 2.7.17.2

**Telnet path:** /Setup/TCP-IP/Loopback-List

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 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).

**SNMP ID:** 2.7.17.3

**Telnet path:** /Setup/TCP-IP/Loopback-List

**Possible values:**

- 0 to max. 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.

**SNMP ID:** 2.7.20

**Telnet 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: 10
- Test-Interval: 10
- Retry-Interval: 1
- Retry-Count: 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.

**Important:** For defined actions that contain a configuration change the trigger interval (fail limit × test interval) should not be less than 5 seconds. Since consecutive triggers lead to consecutive configuration changes a 5 second interval is the minimum supported interval by the device.

**SNMP ID:** 2.7.21

**Telnet path:** /Setup/TCP-IP

## 2.7.21.1 Target-Address

The target address to which the device sends a ping.

**SNMP ID:** 2.7.21.1

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- Valid IP address

## 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.

**Note:** The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

**SNMP ID:** 2.7.21.2

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- 0 to 4294967295 seconds

  **Note:** 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.

**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.

**SNMP ID:** 2.7.21.3

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- 0 to 4294967295

**Note:** 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.

**Default:** 1

**Special values:** 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.

**SNMP ID:** 2.7.21.4

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- 0 to 4294967295

**Note:** 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.

**Default:** 1

**Special values:** 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.

**Note:** The product of the error limit and test interval defines the overall duration until rebooting or executing the action.

**SNMP ID:** 2.7.21.5

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- 0 to 4294967295

**Default:** 10

## 2.7.21.6 Boot-Type

The device executes this action if the ping to the target address was unsuccessful.

**SNMP ID:** 2.7.21.6

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- Warm boot: The device performs a warm boot.
- Cold boot: The device performs a cold boot.
- Action: The device performs a configurable action. Configure the action under `/Setup/TCP-IP/Alive-Test` (also see *Action*).
- Wlan-Mesh: The mesh auto connect feature will be triggered.

**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.

**Note:** 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* ).

**SNMP ID:** 2.7.21.7

**Telnet path:** /Setup/TCP-IP/Alive-Test

**Possible values:**

- 251 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.7.22

**Telnet 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, NetBIOS, etc.) via the network names.

**SNMP ID:** 2.7.30

**Telnet 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, NetBIOS, etc.) can use to reference the network.

**SNMP ID:** 2.7.30.1

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 2.7.30.2 IP-Address

If you use a private address range in your local network, then enter an available 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.

**SNMP ID:** 2.7.30.2

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.7.30.3

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.7.30.4

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Max. 4,094

**Default:** 0

## 2.7.30.5 Interface

Here you select the interface that is to be allocated to the network.

**Note:** The values for 'x' in the list vary per model.

**Telnet path:**

**Setup** > **TCP-IP** > **Network-List**

**Possible values:**

**LAN-1**
**LAN-x**
**WLAN-x-x**
**P2P-x-x**
**BRG-x**

**Default:**

LAN-1

## 2.7.30.6 Source 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.

**SNMP ID:** 2.7.30.6

**Telnet 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.

**SNMP ID:** 2.7.30.7

**Telnet 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 and on the hosts and groups visible to the NetBIOS proxy.

**SNMP ID:** 2.7.30.8

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Maximum 65,535

**Default:** 0

### 2.7.30.9 Comment

You can enter a comment here.

**SNMP ID:** 2.7.30.9

**Telnet path:** /Setup/TCP-IP/Network-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.8 IP-Router

This menu contains the settings for the IP router.

**SNMP ID:** 2.8

**Telnet path:** /Setup

### 2.8.1 Operating

Switches the IP router on or off.

**SNMP ID:** 2.8.1

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Up
- Down

**Default:** Down

### 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.

**SNMP ID:** 2.8.2

**Telnet path:** /Setup/IP-Router

## 2.8.2.1 IP-Address

This is where you specify 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.

**SNMP ID:** 2.8.2.1

**Telnet path:** /Setup/IP-Router/IP-Routing-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 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.

**SNMP ID:** 2.8.2.2

**Telnet path:** /Setup/IP-Router/IP-Routing-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 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.

**SNMP ID:** 2.8.2.3

**Telnet 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.

**SNMP ID:** 2.8.2.4

**Telnet path:** /Setup/IP-Router/IP-Routing-Table

**Possible values:**

- 0 to 16

**Default:** 0

### 2.8.2.5 Masquerading

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.

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 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”.

**Telnet 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.

**SNMP ID:** 2.8.2.6

**Telnet 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.

**SNMP ID:** 2.8.2.7

**Telnet path:** /Setup/IP-Router/IP-Routing-Table

**Possible values:**

- Max. 64 characters

### 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.

**SNMP ID:** 2.8.2.8

**Telnet path:** /Setup/IP-Router/IP-Routing-Table

**Possible values:**

- Maximum 65535

**Default:** 0

**Note:** It follows that the use of routing tags only makes sense in combination with corresponding, decorative rules in the firewall or tagged networks.

## 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.

**SNMP ID:** 2.8.5

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Up
- Down

**Default:** Down

## 2.8.6 Send-ICMP-Redirect

This is where you can chose if ICMP redirects should be sent.

**SNMP ID:** 2.8.6

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Up
- Down

**Default:** Operating

## 2.8.7 Routing-Method

This menu contains the configuration of the routing methods used by your IP router.

**SNMP ID:** 2.8.7

**Telnet path:** /Setup/IP-Router

## 2.8.7.1 Routing method

Controls the analysis of ToS or DiffServ fields.

**Telnet 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.

**SNMP ID:** 2.8.7.2

**Telnet path:** /Setup/IP-Router

**Possible values:**

- normal
- Secured

**Default:** normal

### 2.8.7.3 SYN/ACK-Speedup

Specify if TCP SYN and ACK packets should be given preferential treatment when forwarding.

**SNMP ID:** 2.8.7.3

**Telnet path:** /Setup/IP-Router/Routing-Method

**Possible values:**

- Up
- Down

**Default:** Operating

### 2.8.7.4 L2-L3-Tagging

Specify what should happen with DiffServ layer 2 tags.

**SNMP ID:** 2.8.7.4

**Telnet 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

Specify if DiffServ layer 3 tags should be copied to layer 2.

**SNMP ID:** 2.8.7.5

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Up
- Down

**Default:** Down

### 2.8.7.6 Route-Internal-Services

This is where you select whether the internal services are to be directed via the router.

**SNMP ID:** 2.8.7.6

**Telnet 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

**Note:** 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.

## 2.8.8 RIP

This menu contains the RIP configuration for your IP router.

**SNMP ID:** 2.8.8

**Telnet 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.

**SNMP ID:** 2.8.8.2

**Telnet 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.

**SNMP ID:** 2.8.8.4

**Telnet path:** /Setup/IP-Router/RIP

### 2.8.8.4.1 Peer

Name of the remote station from which WAN RIP packets are to be learned.

**SNMP ID:** 2.8.8.4.1

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

**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_*".

#### 2.8.8.4.2 RIP-Typ

The RIP type details the RIP version with which the local routes are propagated.

**SNMP ID:** 2.8.8.4.2

**Telnet 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.

**SNMP ID:** 2.8.8.4.3

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- On
- Off

**Default:** Off

#### 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.

**SNMP ID:** 2.8.8.4.4

**Telnet 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 touting tag" for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

**SNMP ID:** 2.8.8.4.5

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Maximum 65,535

**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.

**SNMP ID:** 2.8.8.4.6

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Comma-separated list with max. 33 characters

**Default:** Blank

#### 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.

**SNMP ID:** 2.8.8.4.7

**Telnet 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.

**SNMP ID:** 2.8.8.4.8

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- On
- Off

**Default:** Off

**Note:** 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.

### 2.8.8.4.9 Gateway

IP address of the nearest available router in the context of RFC 2091.

**SNMP ID:** 2.8.8.4.9

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

**Special values:** If 0.0.0.0 is entered, the gateway address is determined from PPP negotiation.

**Note:** 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.

**Note:** The device automatically reverts to standard RIP if the gateway indicated does not support RFC 2091.

**Note:** 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

Here you define the filter to be used when receiving RIP packets.

**SNMP ID:** 2.8.8.4.10

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Select from the list of defined RIP filters (max. 16 characters).

**Default:** Blank

### 2.8.8.4.11 Tx-Filter

Here you define the filter to be used when sending RIP packets.

**SNMP ID:** 2.8.8.4.11

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites

**Possible values:**

- Select from the list of defined RIP filters (max. 16 characters).

**Default:** Blank

### 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.

**SNMP ID:** 2.8.8.4.12

**Telnet path:** /Setup/IP-Router/RIP/WAN-Sites/RIP-send

**Possible values**:

- No
- Yes

**Default**: No/Off

### 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

**Telnet path:**
**Setup** > **IP-Router** > **RIP** > **WAN-Table**

**Possible values:**
Specify a valid IPv4 address here.

**Default:**
*empty*

## 2.8.8.5 LAN-Sites

This table is used to adjust RIP settings and to select the network that they apply to.

**SNMP ID:** 2.8.8.5

**Telnet 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.

**SNMP ID:** 2.8.8.5.1

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- Intranet
- DMZ

**Default:** Blank

### 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.

**SNMP ID:** 2.8.8.5.2

**Telnet 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.

**SNMP ID:** 2.8.8.5.3

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- Up
- Down

**Default:** Down

#### 2.8.8.5.4 Propagate

This option defines whether the associated network is to be propagated to other networks.

**SNMP ID:** 2.8.8.5.4

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- Up
- Down

**Default:** Down

#### 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'.

**SNMP ID:** 2.8.8.5.5

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.8.8.5.6

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- Max. 33 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.8.8.5.7

**Telnet path:** /Setup/IP-Router/RIP/LAN-Sites

**Possible values:**

- Up
- Down

**Default:** Down

### 2.8.8.5.10 Rx-Filter

Specify here the filter to be applied when receiving (RX) RIP packets.

**Telnet path:** /Setup/IP-router/RIP/LAN-Sites/Rx-Filter

**Possible values**:

- Max. 16 alphanumerical characters

**Default**: Blank

**Note:** You must first define the filter in the RIP filter list in order to use it here.

### 2.8.8.5.11 Tx-Filter

Specify here the filter to be applied when sending (TX) RIP packets.

**Telnet path:** /Setup/IP-router/RIP/LAN-Sites/Tx-Filter

**Possible values**:

- Max. 16 alphanumerical characters

**Default**: Blank

**Note:** You must first define the filter in the RIP filter list in order to use it here.

#### 2.8.8.5.12 RIP-send

Specify here whether routes should be propagated in this network. The RIP type must also be set.

**Telnet path:** /Setup/IP router/RIP/LAN-Sites/RIP-Send

**Possible values**:

- No
- Yes

**Default**: No

### 2.8.8.6 Parameter

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.

**SNMP ID:** 2.8.8.6

**Telnet 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.

**SNMP ID:** 2.8.8.6.1

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 10 to 99 seconds

**Default:** 30 seconds

#### 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.

**SNMP ID:** 2.8.8.6.2

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.8.8.6.3

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.8.8.6.4

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.8.8.6.5

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 1 to 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.

**SNMP ID:** 2.8.8.6.6

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 16 to 99

**Default:** 16

#### 2.8.8.6.7 Routes-per-Frame

The number of routes that can be propagated in a single packet.

**SNMP ID:** 2.8.8.6.7

**Telnet path:** /Setup/IP-Router/RIP/Parameter

**Possible values:**

- 1 to 90

**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.

**Telnet 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.

**SNMP ID:** 2.8.8.7

**Telnet path:** /Setup/IP-Router/RIP

### 2.8.8.7.1 Name

Name of the filter.

**SNMP ID:** 2.8.8.7.1

**Telnet path:** /Setup/IP-Router/RIP/Filter

**Possible values:**

- 18 characters

**Note:** 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.

### 2.8.8.7.2 Filter

Comma-separated list of networks that are to be accepted (+) or rejected (-).

**SNMP ID:** 2.8.8.7.2

**Telnet path:** /Setup/IP-Router/RIP/Filter

**Possible values:**

- 64 characters from ,+-/0123456789.

**Note:** The plus-sign for accepted networks is optional.

**Note:** 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.

## 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
- Remote site
- Port
- VLAN-ID
- Network name

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

### 2.8.8.8.3 Time

The time required to reach the network via this route.

**Telnet 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).

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.8.8 Peer

Remote device that can be reached over this route.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.8.11 Network name

The name of the network to which the route belongs.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.8.12 Port

The (logical) LAN interface via which the route was learned.

**Telnet 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
- Remote site
- Port
- VLAN-ID
- Network name

**Telnet path:** /Setup/IP-Router/RIP/All-Routes

#### 2.8.8.9.1 IP-Address

The IP address of the network to which the route belongs.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.9.3 Time

The time required to reach the network via this route.

**Telnet 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).

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.9.8 Peer

Remote device that can be reached over this route.

**Telnet 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.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.9.11 Network name

The name of the network to which the route belongs.

**Telnet path:**

**Setup** > **IP-Router** > **RIP** > **Best-Routes**

#### 2.8.8.9.12 Port

The (logical) LAN interface via which the route was learned.

**Telnet 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.

**SNMP ID:** 2.8.9

**Telnet path:** /Setup/IP-Router

## 2.8.9.1 TCP-Aging-Seconds

Specify here how long an IPsec connection is inactive before the corresponding entry in the masquerading table is deleted.

**SNMP ID:** 2.8.9.1

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- 0 to 65,535

**Default:** 300 seconds

## 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.

**SNMP ID:** 2.8.9.2

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- 0 to 65,535

**Default:** 20 seconds

## 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.

**SNMP ID:** 2.8.9.3

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- 0 to 65,535

**Default:** 10 seconds

## 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.

**SNMP ID:** 2.8.9.4

**Telnet path:** /Setup/IP-Router/1-N-NAT

### 2.8.9.4.1 D-port-from

Specify the port of the desired service here.

**SNMP ID:** 2.8.9.4.1

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Maximum 65,535

**Default:** 0

### 2.8.9.4.2 Intranet-Address

Enter the address of the computer in the intranet providing the service.

**SNMP ID:** 2.8.9.4.2

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.9.4.3 D-Port-to

Specify the port of the desired service here.

**SNMP ID:** 2.8.9.4.3

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Maximum 65,535

**Default:** 0

### 2.8.9.4.4 Map-Port

Port used for forwarding the packet.

**SNMP ID:** 2.8.9.4.4

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Maximum 65,535

**Default:** 0

### 2.8.9.4.5 Active

You can set this entry temporarily inactive without having to delete it.

**SNMP ID:** 2.8.9.4.5

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Up
- Down

**Default:** Operating

### 2.8.9.4.6 Comment

This field is available for comments.

**SNMP ID:** 2.8.9.4.6

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Max. 64 characters

**Default:** /

### 2.8.9.4.7 Peer

Remote site which is valid for this entry.

**SNMP ID:** 2.8.9.4.7

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Select from the list of defined peers.

### 2.8.9.4.8 Protocol

Here you define which protocol the dataset applies to.

**SNMP ID:** 2.8.9.4.8

**Telnet 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.

**SNMP ID:** 2.8.9.4.9

**Telnet path:** /Setup/IP-Router/1-N-NAT/Service-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.9.5 Table-1-N-NAT

The 1-N-NAT table shows the masked connections.

**SNMP ID:** 2.8.9.5

**Telnet path:** /Setup/IP-Router/1-N-NAT

#### 2.8.9.5.1 Intranet-Address

Shows the internal IP address of the station to which a masked connection has been stored.

**SNMP ID:** 2.8.9.5.1

**Telnet path:** /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

**Possible values:**

- Valid IP address

#### 2.8.9.5.2 S-Port

Source port of the masked connection.

**SNMP ID:** 2.8.9.5.2

**Telnet 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.

**SNMP ID:** 2.8.9.5.3

**Telnet 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).

**SNMP ID:** 2.8.9.5.4

**Telnet path:** /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

#### 2.8.9.5.5 Handler

Handler required for masking, e.g. FTP

**SNMP ID:** 2.8.9.5.5

**Telnet path:** /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

#### 2.8.9.5.6 Remote-Address

Remote IP address that the masked connection was connected to.

**SNMP ID:** 2.8.9.5.6

**Telnet path:** /Setup/IP-Router/1-N-NAT/Table-1-N-NAT

**Possible values:**

- Valid IP address

### 2.8.9.6 Fragments

This setting controls the firewall's behavior regarding fragmented IP packets.

**SNMP ID:** 2.8.9.6

**Telnet 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.

**SNMP ID:** 2.8.9.7

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- 1 to 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.

**SNMP ID:** 2.8.9.8

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- 0 to 65,535

**Default:** 2000

## 2.8.9.9 IPSec-Table

The IPSec table displays the masked IPSec connections, including some of the connection parameters.

**SNMP ID:** 2.8.9.9

**Telnet path:** /Setup/IP-Router/1-N-NAT

### 2.8.9.9.1 Remote-Address

Address of the remote VPN gateway

**SNMP ID:** 2.8.9.9.1

**Telnet path:** /Setup/IP-Router/1-N-NAT/IPSec-Table

**Possible values:**

- Valid IP address

### 2.8.9.9.2 local-Address

Address of the local VPN gateway (generally a VPN client in the local network)

**SNMP ID:** 2.8.9.9.2

**Telnet path:** /Setup/IP-Router/1-N-NAT/IPSec-Table

**Possible values:**

- Valid IP address

### 2.8.9.9.3 rc-hi

The most significant 32 bits of the IKE cookie of the remote VPN gateway

**SNMP ID:** 2.8.9.9.3

**Telnet 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

**SNMP ID:** 2.8.9.9.4

**Telnet 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

**SNMP ID:** 2.8.9.9.5

**Telnet 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

**SNMP ID:** 2.8.9.9.6

**Telnet path:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.7 remote-SPI

SPI used by the remote VPN gateway

**SNMP ID:** 2.8.9.9.7

**Telnet path:** /Setup/IP-Router/1-N-NAT/IPSec-Table

#### 2.8.9.9.8 local-SPI

SPI used by the local VPN gateway

**SNMP ID:** 2.8.9.9.8

**Telnet 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 divided into IPsec aging seconds. The default value is 2000 seconds

**SNMP ID:** 2.8.9.9.9

**Telnet 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 waiting for SPI

0x04 Other connections waiting for SPI

0x08 Aggressive mode connection

0x10 NAT-Traversal-Connection

0x20 Session recovery

**SNMP ID:** 2.8.9.9.10

**Telnet 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

**SNMP ID:** 2.8.9.9.11

**Telnet 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

**SNMP ID:** 2.8.9.9.12

**Telnet 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.

**SNMP ID:** 2.8.9.9.13

**Telnet 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.

**SNMP ID:** 2.8.9.9.14

**Telnet 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.

**SNMP ID:** 2.8.9.10

**Telnet path:** /Setup/IP-Router/1-N-NAT

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.8.10 Firewall

This menu contains the firewall configuration.

**SNMP ID:** 2.8.10

**Telnet 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 areas, e.g. HTTP, Mail&News, FTP, ...)

**SNMP ID:** 2.8.10.1

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.1.1 Name

Specify here a unique name for this object.

**SNMP ID:** 2.8.10.1.1

**Telnet path:** /Setup/IP-Router/Firewall/Objects

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.8.10.1.2 Description

**SNMP ID:** 2.8.10.1.2

**Telnet path:** /Setup/IP-Router/Firewall/Objects

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.

**Possible values:**

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

| *Description* | *Object-ID* | *Examples and comments* |
|---|---|---|
| Local network | %L | |
| remote sites | %H | Name must be in DSL/PPTP or VPN remote site list |
| Host name | %D | |
| MAC address | %E | 00:A0:57:01:02:03 |

| *Description* | *Object-ID* | *Examples and comments* |
|---|---|---|
| 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) |

*Table 9: Objects for firewall actions*

**Note:** 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.

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

**Default:** Blank

## 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.

HiLCOS 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 HiLCOS 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 HiLCOS syntax (e.g. %P6 for TCP).

**SNMP ID:** 2.8.10.2

**Telnet path:** /Setup/IP-Router/Firewall

**Note:** 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 HiLCOS syntax, the same rules apply as specified in the following sections for protocols, source/destination and firewall actions.

### 2.8.10.2.1 Name

Specify here a unique name for this firewall rule.

**SNMP ID:** 2.8.10.2.1

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.8.10.2.2 Protocol

Specification of the protocols for which this entry is to apply.

**SNMP ID:** 2.8.10.2.2

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Direct entry in HiLCOS syntax as described in the *Objects* table.
- Link to an entry of the object table.

**Default:** Blank

### 2.8.10.2.3 Source

Specification of the source stations for which this entry is to apply.

**SNMP ID:** 2.8.10.2.3

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Direct entry in HiLCOS syntax as described in the *Objects* table.
- Link to an entry of the object table.

**Default:** Blank

### 2.8.10.2.4 Destination

Specification of the destination stations for which this entry is to apply.

**SNMP ID:** 2.8.10.2.4

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Direct entry in HiLCOS syntax as described in the *Objects* table.
- Link to an entry of the object table.

**Default:** Blank

### 2.8.10.2.7 Action

Action to be run if the firewall rule applies to a packet.

**SNMP ID:** 2.8.10.2.7

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Direct entry in HiLCOS syntax as described in the *Actions* table.
- Link to an entry of the action table.

**Default:** Blank

### 2.8.10.2.8 Linked

Links the rule to other rules.

**SNMP ID:** 2.8.10.2.8

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Yes
- No

**Default:** No

### 2.8.10.2.9 Priority

Priority of the rule.

**SNMP ID:** 2.8.10.2.9

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- 0 to 255

**Default:** Blank

### 2.8.10.2.10 Active

Switches the rule on/off.

**SNMP ID:** 2.8.10.2.10

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.8.10.2.11 VPN-Rule

Activates the rule for creating VPN rules.

**SNMP ID:** 2.8.10.2.11

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Yes
- No

**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.

**SNMP ID:** 2.8.10.2.12

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.8.10.2.13 Comment

Comment for this entry.

**SNMP ID:** 2.8.10.2.13

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.8.10.2.14 Rtg-Tag

Routing tag for the rule.

**SNMP ID:** 2.8.10.2.14

**Telnet path:** /Setup/IP-Router/Firewall/Rules

**Possible values:**

- 0 to 65535

**Default:** 0

### 2.8.10.2.15 Source 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.

**Telnet path:**

**Setup** > **IP-Router** > **Firewall** > **Rules**

**Possible values:**

0 to 65535

**Comment**

- 65535: The firewall rule is applied if the expected interface- or routing tag is 0.
- 1…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).

**Default:**

0

## 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..

**SNMP ID:** 2.8.10.3

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.3.1 Index

Index for this entry in the list.

**SNMP ID:** 2.8.10.3.1

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.2 Protocol

TCP protocol for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.2

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.3 Src-Address

Source IP address for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.3

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

**Possible values:**

- Valid IP address

### 2.8.10.3.4 Source netmask

Source IP netmask for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.4

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

**Possible values:**

- Valid IP address

### 2.8.10.3.5 S-St.

Start address of range of source IP addresses whose data packets are processed by this entry.

**SNMP ID:** 2.8.10.3.5

**Telnet 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.

**SNMP ID:** 2.8.10.3.6

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.7 Dst-Address

Destination IP address for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.7

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

**Possible values:**

- Valid IP address

### 2.8.10.3.8 Dst-netmask

Destination IP netmask for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.8

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

**Possible values:**

- Valid IP address

### 2.8.10.3.9 D-St.

Start address of range of destination IP addresses whose data packets are processed by this entry.

**SNMP ID:** 2.8.10.3.9

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.10 D-End

Finish address of range of destination IP addresses whose data packets are processed by this entry.

**SNMP ID:** 2.8.10.3.10

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.11 Action

Action performed for the data packets processed by this entry.

**SNMP ID:** 2.8.10.3.11

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.13 Source MAC

Source MAC address for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.13

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.14 Dst-MAC

Destination MAC address for data packets processed by this entry.

**SNMP ID:** 2.8.10.3.14

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

### 2.8.10.3.15 Linked

Indicates whether further firewall rules are applied after this action.

**SNMP ID:** 2.8.10.3.15

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

#### 2.8.10.3.16 Priority

Priority for this entry.

**SNMP ID:** 2.8.10.3.16

**Telnet 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.

**SNMP ID:** 2.8.10.3.17

**Telnet path:** /Setup/IP-Router/Firewall/Filter-List

#### 2.8.10.3.18 Source tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received.

**Telnet path:**

**Setup** > **IP-Router** > **Firewall** > **Filter-List**

### 2.8.10.4 Actions

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.

**SNMP ID:** 2.8.10.4

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.4.1 Name

Specify a unique name for this action.

**SNMP ID:** 2.8.10.4.1

**Telnet path:** /Setup/IP-Router/Firewall/Actions

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.8.10.4.2 Description

**SNMP ID:** 2.8.10.4.2

**Telnet path:** /Setup/IP-Router/Firewall/Actions

In the actions table, firewall actions are combined as any combination of conditions, limits, packet actions and other measures.

**Possible values:**

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.

#### Conditions

| *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` |

| Condition | Description | Object-ID |
|---|---|---|
| VPN-Filter | The filter is active if the packet was received, or is to be sent, via a VPN connection | @v |

*Table 10: Conditions for firewall actions*

**Note:** 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:

- Relation: connection-related (c) or global (g)
- Type: Data rate (d), number of packets (p), or packet rate (b)
- Limit value
- Other parameters (e.g., time and size)

The following limits are available:

| Limit | Description | Object-ID |
|---|---|---|
| Data (abs) | Absolute number of kilobytes over the connection, after which the action is performed | %lcd |
| Data (rel) | Number of kilobytes per second, minute, hour over the connection, after which the action is performed | %lcds, %lcdm, %lcdh |
| Packet (abs) | Absolute number of packets over the connection, after which the action is performed | %lcp |
| Packet (rel) | Number of packets per second, minute, hour, or absolute over the connection, after which the action is performed | %lcps, %lcpm, %lcph |
| Global data (abs) | Absolute number of kilobytes sent to or received from the destination computer, after which the action is performed | %lgd |

| *Limit* | *Description* | *Object-ID* |
|---|---|---|
| Global data (rel) | Number of kilobytes per second, minute, or hour sent to or received from the destination computer, after which the action is performed | `%lgds`, `%lgdm`, `%lgdh` |
| Global packet (abs) | Absolute number of packets sent to or received from the destination computer, after which the action is performed | `%lgp` |
| Global packet (rel) | Number of packets per second, minute, or hour sent to or received from the destination computer, after which the action is performed | `%lgps`, `%lgpm`, `%lgph` |
| Receive option | Limit applies to the receive direction only (in combination with the above limitations). Examples are given in the object ID column | `%lgdsr`, `%lcdsr` |
| Transmit option | Limit applies to the transmit direction only (in combination with the above limitations). Examples are given in the object ID column | `%lgdst`, `%lcdst` |

*Table 11: Limits for firewall actions*

**Note:** If an action is specified without a limit, a packet limit is used that is immediately exceeded on the first packet.

### Quality-of-Service-Objects

Another limit object is the Quality-of-service object (or QoS object) that allows you to define a minimum throughput or a minimum bandwidth, either per connection or globally. It is possible to specify any of the limits that apply to the normal limit objects, such as connection-related or global minimums, absolute or time-dependent (relative) minimums, and packet- or data-related minimums. The same conventions apply as for the limit objects.

QoS objects are invoked by the token %q, and they are only different from limit objects in that they initially have an implicit "accept" action, i.e. after the threshold has been exceeded the packets that follow are still accepted.

- All packets that pass through a filter with a QoS object are transmitted preferentially by the device (corresponding to a 'low delay' flag set in the TOS field of the IP header) as long as the quantity of transmitted packets or data is less than the specified threshold.

- If the threshold is exceeded, the actions behind the QoS object are executed. This combination of QoS and limit objects can be used to set a minimum and maximum bandwidth for a service.

For example, the description below results in a minimum bandwidth of 32 kbps per connection and a maximum bandwidth of 256 kbps for all connections:

```
%a %qcds32%a %lgds256%d
```

In this case we can avoid explicitly specifying the accept action, either as the main action or as the triggered action, and the description be abbreviated as follows:

```
%qcds32 %lgds256%d
```

If the minimum and maximum bandwidths of a channel should be the same, then the drop action can be specified directly in the QoS object (abbreviated notation):

```
%qcds32%d
```

In this case, a minimum bandwidth of 32 kbps is reserved and, at the same time, all packets that are to be transmitted above this bandwidth are dropped. This formulation is thus synonymous with `%a %qcds32%a %lgds32%d`.

The following objects are available:

| *QoS object* | *Description* | *Object-ID* |
|---|---|---|
| Reserve minimum and maximum bandwidth | Reserves the specified bandwidth according to the other parameters, either globally or per connection | `%q` |
| Force minimum or maximum bandwidth | Forces the specified bandwidth. If the requested bandwidth is unavailable, the device refuses the connection. | `%qf` |

*Table 12: QoS objects for firewall actions*

### Packet actions

| *Packet action* | *Description* | *Object-ID* |
|---|---|---|
| Accept | The packet is accepted. | `%a` |
| Reject | The packet is rejected with a corresponding error message. | `%r` |
| Drop | The packet is dropped silently. | `%d` |

| *Packet action* | *Description* | *Object-ID* |
|---|---|---|
| External check | The packet is passed another module for an external check. The %x follows the identifier of the module performing the check. Possible values:<br>▶ %xc for the content filter, followed by a previously defined content-filter profile, e.g. %xcCF-BASIC-PROFILE. | %x |

*Table 13: Packet actions for firewall actions*

**Note:** These packet actions can be combined with one another in any way. For nonsensical or ambiguous actions (such as Accept + Drop), the more secure one is taken - “Drop" in this example.

### Other measures

Apart from packet actions, the firewall can perform other actions once the limits have been reached. For example, the firewall can send notifications over various channels, or block ports or hosts for a certain period.

The following measures are available:

| *Countermeasures* | *Description* | *Object-ID* |
|---|---|---|
| Syslog | Provides a detailed message via Syslog. | %s |
| E-mail | Sends an e-mail to the administrator. | %m |
| SNMP | Sends an SNMP trap | %n |
| Close port | Closes the destination port of the packet for a configurable time | %p |
| Deny host | Blocks the sender address of the packet for a configurable time | %h |
| Disconnect | Disconnects the physical connection to the remote site over which the packet was received or is to be sent. | %t |
| Zero-limit | Resets the limit counter (see below) to 0 when the trigger threshold is exceeded | %z |

| *Countermeasures* | *Description* | *Object-ID* |
|---|---|---|
| Fragmentation | Forces the fragmentation of all packets not matching the rule. | %f |

*Table 14: Other measures for firewall actions*

**Note:** When the “Close port” action is run, an entry is made in a block list with which all packets sent to the respective computer and port are dropped. For the “Close port” object, a block time in seconds, minutes or hours can be specified. This is noted directly behind the object ID. This time is made up of the identifier for the time unit (h, m, s for hour, minute, second) as well as the actual time specification. For example, %pm10 blocks the port for 10 minutes. "Minutes" is used as the unit if no time unit is specified. (%p10 is therefore equivalent to %pm10)

**Note:** If the “Deny host” action is run, the sender of the packet is entered into a block list. From this moment on, all packets received from the blocked computer are dropped. The "Deny host” object can also be given a block time, formed as described for the “Close port” option.

**Note:** The "fragmentation" action can be applied directionally (e.g. %ft512 fragments transmitted packets and %fr512 fragments received packets to 512 bytes) or, instead of hard fragmentation, it can reduce the PTMU only (%fp512 reduces the PMTU to 512 bytes). The PMTU reduction can also be defined depending on direction (%fpt512, %fpr512). The "Fragmentation" action applies at all times, irrespective of whether a limit has been exceeded or not.

**Default:** Blank

## 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".

**SNMP ID:** 2.8.10.5

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.5.1 Src-Address

IP address of the station that established a connection.

**SNMP ID:** 2.8.10.5.1

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

**Possible values:**

- Valid IP address

### 2.8.10.5.2 Dst-Address

Destination IP address to which a connection was established.

**SNMP ID:** 2.8.10.5.2

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

**Possible values:**

- Valid IP address

### 2.8.10.5.3 Protocol

Protocol allowed on this connection.

**SNMP ID:** 2.8.10.5.3

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

### 2.8.10.5.4 Source port

Source port of the station that established a connection.

**SNMP ID:** 2.8.10.5.4

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

### 2.8.10.5.5 Dst-Port

Destination port to which a connection was established.

**SNMP ID:** 2.8.10.5.5

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

### 2.8.10.5.6 Timeout

Lease for this entry in the table.

**SNMP ID:** 2.8.10.5.6

**Telnet 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. This is the case with H.323, for example).

**Telnet path:**/Setup/IP-Router/Firewall/Connection-List

**Possible values:**

- 00000001 TCP: SYN sent
- 00000002 TCP: SYN/ACK received
- 00000004 TCP: Wait for ACK from server
- 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: Associated 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.

**SNMP ID:** 2.8.10.5.8

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

#### 2.8.10.5.9 Source route

Source route used to establish this connection.

**SNMP ID:** 2.8.10.5.9

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

#### 2.8.10.5.10 Dest-Route

Destination route to which a connection was established.

**SNMP ID:** 2.8.10.5.10

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

#### 2.8.10.5.11 Rtg-tag

Connection routing tag.

**SNMP ID:** 2.8.10.5.11

**Telnet path:** /Setup/IP-Router/Firewall/Connection-List

## 2.8.10.6 Host block 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.

**SNMP ID:** 2.8.10.6

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.6.1 Src-Address

Source IP address that is blocked by this entry.

**SNMP ID:** 2.8.10.6.1

**Telnet path:** /Setup/IP-Router/Firewall/Host-Block-List

**Possible values:**

- Valid IP address

### 2.8.10.6.2 Timeout

Lease for this entry in the table.

**SNMP ID:** 2.8.10.6.2

**Telnet path:** /Setup/IP-Router/Firewall/Host-Block-List

### 2.8.10.6.3 Filter rule

Shows the filter rule that generated the entry.

**SNMP ID:** 2.8.10.6.3

**Telnet path:** /Setup/IP-Router/Firewall/Host-Block-List

## 2.8.10.7 Port block 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.

**SNMP ID:** 2.8.10.7

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.7.1 Dst-Address

Destination IP address that is blocked by this entry.

**SNMP ID:** 2.8.10.7.1

**Telnet path:** /Setup/IP-Router/Firewall/Port-Block-List

**Possible values:**

- Valid IP address

### 2.8.10.7.2 Protocol

Protocol that is blocked by this entry.

**SNMP ID:** 2.8.10.7.2

**Telnet path:** /Setup/IP-Router/Firewall/Port-Block-List

### 2.8.10.7.3 Dst-Port

Destination port blocked by this entry.

**SNMP ID:** 2.8.10.7.3

**Telnet path:** /Setup/IP-Router/Firewall/Port-Block-List

### 2.8.10.7.4 Timeout

Lease for this entry in the table.

**SNMP ID:** 2.8.10.7.4

**Telnet path:** /Setup/IP-Router/Firewall/Port-Block-List

### 2.8.10.7.5 Filter rule

Shows the filter rule that generated the entry.

**SNMP ID:** 2.8.10.7.5

**Telnet 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.

**SNMP ID:** 2.8.10.8

**Telnet path:** /Setup/IP-Router/Firewall

**Possible values:**

- 100 to 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).

**SNMP ID:** 2.8.10.9

**Telnet 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.

**SNMP ID:** 2.8.10.10

**Telnet path:** /Setup/IP-Router/Firewall

**Possible values:**

- Max. 255 characters

**Note:** For e-mail messaging, you have to enter the necessary settings into the main group "Log & Trace" in the subsection "SMTP".

## 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.

**SNMP ID:** 2.8.10.11

**Telnet path:** /Setup/IP-Router/Firewall

**Possible values:**

- Up
- Down

**Default:** Operating

**Note:** Defined VPN rules continue to be observed even with the firewall switched off.

## 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.

**SNMP ID:** 2.8.10.12

**Telnet path:** /Setup/IP-Router/Firewall

**Possible values:**

- 50 to 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).

**SNMP ID:** 2.8.10.13

**Telnet 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).

**SNMP ID:** 2.8.10.14

**Telnet 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).

**SNMP ID:** 2.8.10.15

**Telnet 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.

**SNMP ID:** 2.8.10.16

**Telnet path:** /Setup/IP-Router/Firewall

**Possible values:**

- Up
- Down

**Default:** Down

## 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.

**SNMP ID:** 2.8.10.17

**Telnet 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.

**SNMP ID:** 2.8.10.19

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.19.1 Src-Address

Source IP address that can be used by the open ports and protocols in this entry.

**SNMP ID:** 2.8.10.19.1

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

**Possible values:**

- Valid IP address

### 2.8.10.19.2 Dst-Address

Destination IP address to which a connection may be established using the open ports and protocols in this entry.

**SNMP ID:** 2.8.10.19.2

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

**Possible values:**

- Valid IP address

#### 2.8.10.19.3 Protocol

Protocol opened by this entry.

**SNMP ID:** 2.8.10.19.3

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

#### 2.8.10.19.5 Dst-Port

Destination port opened by this entry.

**SNMP ID:** 2.8.10.19.5

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

#### 2.8.10.19.6 Timeout

Lease for this entry in the table.

**SNMP ID:** 2.8.10.19.6

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

#### 2.8.10.19.8 Filter rule

Shows the filter rule that generated the entry.

**SNMP ID:** 2.8.10.19.8

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

#### 2.8.10.19.9 Source route

Source route used to establish this connection.

**SNMP ID:** 2.8.10.19.9

**Telnet path:** /Setup/IP-Router/Firewall/Open-Port-List

### 2.8.10.20 Applications

This menu contains the configuration of individual firewall applications.

**SNMP ID:** 2.8.10.20

**Telnet path:** /Setup/IP-Router/Firewall

### 2.8.10.20.1 FTP

This menu contains the configuration of FTP for your firewall.

**SNMP ID:** 2.8.10.20.1

**Telnet 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.

**SNMP ID:** 2.8.10.20.1.1

**Telnet path:** /Setup/IP-Router/Firewall/Applications/FTP

**Possible values:**

- Off
- Always
- WAN
- Default route

**Default:** No

#### *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.

**SNMP ID:** 2.8.10.20.1.2

**Telnet 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.

**SNMP ID:** 2.8.10.20.1.3

**Telnet path:** /Setup/IP-Router/Firewall/Applications/FTP

**Possible values:**

- 1024 to 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.

**SNMP ID:** 2.8.10.20.1.4

**Telnet 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.

**SNMP ID:** 2.8.10.20.1.5

**Telnet 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.

**SNMP ID:** 2.8.10.20.2

**Telnet 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.

**SNMP ID:** 2.8.10.20.2.1

**Telnet 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.

**SNMP ID:** 2.8.10.20.2.2

**Telnet 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.

**SNMP ID:** 2.8.10.20.2.3

**Telnet path:** /Setup/IP-Router/Firewall/Applications/IRC

**Possible values:**

- 1024 to 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.

**SNMP ID:** 2.8.10.20.2.4

**Telnet 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.

**SNMP ID:** 2.8.10.20.10

**Telnet 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.

**SNMP ID:** 2.8.11

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.12 End-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.

**SNMP ID:** 2.8.12

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.13 Default-Time-List

Time-dependent control allows you to specify different destinations for the default route depending on the day of the week and time.

**SNMP ID:** 2.8.13

**Telnet path:** /Setup/IP-Router

## 2.8.13.1 Index

Index for this entry in the list.

**SNMP ID:** 2.8.13.1

**Telnet path:** /Setup/IP-Router/Default-Time-List

## 2.8.13.2 Days

Specify the days when this entry should be used.

**SNMP ID:** 2.8.13.2

**Telnet path:** /Setup/IP-Router/Default-Time-List

**Possible values:**

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

- Holiday

**Default:** No days are marked

## 2.8.13.3 Start

Used to specify the time period during which this entry should be used.

**SNMP ID:** 2.8.13.3

**Telnet path:** /Setup/IP-Router/Default-Time-List

**Possible values:**

- 12:00 AM to 11:59 PM (CET)

**Default:** 0

## 2.8.13.4 Stop

Used to specify the time period during which this entry should be used.

**SNMP ID:** 2.8.13.4

**Telnet path:** /Setup/IP-Router/Default-Time-List

**Possible values:**

- 12:00 AM to 11:59 PM (CET)

**Default:** 0.999305556

## 2.8.13.5 Peer

The remote site specified here will become the default route after this entry becomes valid when the defined time period is reached. Here you select the name of a remote site from the list of remote sites.

**SNMP ID:** 2.8.13.5

**Telnet path:** /Setup/IP-Router/Default-Time-List

**Possible values:**

- Select from the list of defined peers.

### 2.8.14 Usage-Default-Timetable

Activates the time-dependent control of the default route. The default route is normally used to establish the connection to an Internet provider. The time control allows you to select various Internet providers depending on the time, for example to benefit from the most favorable provider at a certain time of day.

**SNMP ID:** 2.8.14

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Up
- Down

**Default:** Down

**Note:** To make use of this mechanism, a default route must have been specified in the routing table. The router specified in the default route is only used during those times that are not covered by the timed control table.

### 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.

**SNMP ID:** 2.8.19

**Telnet path:** /Setup/IP-Router

## 2.8.19.1 Idx.

Unique index for the entry

**SNMP ID:** 2.8.19.1

**Telnet path:** /Setup/IP-Router/N-N-NAT

**Possible values:**

- Max. 4 characters

**Default:** Blank

## 2.8.19.2 Src-Address

IP address of the computer or network that is to receive an alternative IP address.

**SNMP ID:** 2.8.19.2

**Telnet path:** /Setup/IP-Router/N-N-NAT

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.8.19.3 Src-Mask

Netmask of the source range.

**SNMP ID:** 2.8.19.3

**Telnet path:** /Setup/IP-Router/N-N-NAT

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.8.19.4 Dst-Station

Name of the remote device that can be used to access the remote network.

**SNMP ID:** 2.8.19.4

**Telnet path:** /Setup/IP-Router/N-N-NAT

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

### 2.8.19.5 Mapped-Network

IP addresses or address range to be used for translation.

**SNMP ID:** 2.8.19.5

**Telnet path:** /Setup/IP-Router/N-N-NAT

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

**Note:** 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.

**Note:** The address range for translation must be at least as large as the source address range.

**Note:** Please note that the N:N mapping function is only effective when the firewall is activated.

## 2.8.20 Load-Balancer

This menu contains the configuration of load balancing for your IP router.

**SNMP ID:** 2.8.20

**Telnet path:** /Setup/IP-Router

## 2.8.20.1 Operating

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.

**SNMP ID:** 2.8.20.1

**Telnet path:** /Setup/IP-Router/Load-Balancer

**Possible values:**

- Up
- Down

**Default:** Down

## 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.

**SNMP ID:** 2.8.20.2

**Telnet path:** /Setup/IP-Router/Load-Balancer

### 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.

**SNMP ID:** 2.8.20.2.1

**Telnet path:** /Setup/IP-Router/Load-Balancer/Bundle-Peers

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

#### 2.8.20.2.2 Bundle-Peer-1

Name of a previously configured remote site to which the others are to be bundled.

**SNMP ID:** 2.8.20.2.2

**Telnet path:** /Setup/IP-Router/Load-Balancer/Bundle-Peers

**Possible values:**

- Max. 16 characters

**Default:** Blank

#### 2.8.20.2.3 Bundle-Peer-2

Name of a previously configured remote site to which the others are to be bundled.

**SNMP ID:** 2.8.20.2.3

**Telnet path:** /Setup/IP-Router/Load-Balancer/Bundle-Peers

**Possible values:**

- Max. 16 characters

**Default:** Blank

#### 2.8.20.2.4 Bundle-Peer-3

Name of a previously configured remote site to which the others are to be bundled.

**SNMP ID:** 2.8.20.2.4

**Telnet path:** /Setup/IP-Router/Load-Balancer/Bundle-Peers

**Possible values:**

- Max. 16 characters

**Default:** Blank

#### 2.8.20.2.5 Bundle-Peer-4

Name of a previously configured remote site to which the others are to be bundled.

**SNMP ID:** 2.8.20.2.5

**Telnet path:** /Setup/IP-Router/Load-Balancer/Bundle-Peers

**Possible values:**

- Max. 16 characters

**Default:** Blank

#### 2.8.20.2.10 Client binding

Here you enable or disable the client binding for each load balancer.

**Telnet path:**

**Setup** > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

**Possible values:**

**Yes**

Client binding is enabled.

**No**

Client binding is disabled.

**Default:**

No

### 2.8.20.3 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.

**Telnet 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.

**Note:** The table already contains the default entries

- HTTPS
- HTTP
- ANY

**Telnet path:**

**Status** > **IP-Router** > **Load-Balancer** > **Client-Binding**

### *2.8.20.3.1.1 Name*

Enter a descriptive name for this entry.

**Telnet 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.

**Note:** Learn more about IP protocol numbers in the *online database* of the IANA.

**Telnet 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.

**Telnet 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.

**Telnet 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 Binding minutes

Specify the time in minutes for the binding entries to be valid for a client.

**Telnet path:**

**Status** > **IP-Router** > **Load-Balancer** > **Client-Binding**

**Possible values:**

Max. 3 characters from `[0-999]`

**Special values:**

**0**

**Default:**

30

### 2.8.20.3.3 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.

**Telnet 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

### 2.8.21 VRRP

This menu contains the configuration of VRRP for your IP router.

**SNMP ID:** 2.8.21

**Telnet path:** /Setup/IP-Router

## 2.8.21.1 Operating

VRRP – 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.

**SNMP ID:** 2.8.21.1

**Telnet path:** Setup/IP-Router/VRRP

**Possible values:**

- Up
- Down

**Default:** Down

## 2.8.21.2 VRRP-List

In the VRRP list you can define and configure virtual routers.

**SNMP ID:** 2.8.21.2

**Telnet path:** Setup/IP-Router/VRRP

### 2.8.21.2.1 Router-ID

Unique ID for the virtual router.

**SNMP ID:** 2.8.21.2.1

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- 0 to 255

**Default:** 1

### 2.8.21.2.2 virt.-Address

IP address for the virtual router. All routers on which the virtual router is set up must assign this router the same IP address.

**SNMP ID:** 2.8.21.2.2

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.21.2.3 Prio

Main priority for the virtual router. Values between 0 and 255 are permitted. Priority is proportional to the value entered. The values 0 and 255 have special meanings. '0' turns the virtual router off. '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to

the router. If this is not the case, the router will be reported by all other routers in their event logs.

**SNMP ID:** 2.8.21.2.3

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- 0 to 255

**Default:** 0

### 2.8.21.2.4 B-Prio

Backup priority for the virtual router. Values between 0 and 255 are permitted. Priority is proportional to the value entered. The values 0 and 255 have special meanings. 0 disables the virtual router in the event of backup. Checks are conducted regularly in order to determine whether the standard connection can be reestablished. The interval is determined by the Reconnect-Delay parameter. '255' is only accepted when the virtual router address is identical to the address of the interface that is connected to the router. If this is not the case, the router will be reported by all other routers in their event logs. When the backup connection cannot be established in backup mode, then the virtual router switches completely to the standby mode and attempts to reestablish the standard or backup connection at regular intervals.

**SNMP ID:** 2.8.21.2.4

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- 0 to 255

**Default:** 0

### 2.8.21.2.5 Peer

The entry for the name of the remote site is optional. If a peer name is entered here it will be controlled by VRRP. If, for example, the peer loses its Internet connection backup mode kicks in. If no peer is entered, VRRP can be used to cover a hardware outage. The remote site can still also be assigned to other virtual routers.

**SNMP ID:** 2.8.21.2.5

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

#### 2.8.21.2.6 Comment

This is where you can insert a comment to describe the virtual router.

**SNMP ID:** 2.8.21.2.6

**Telnet path:** /Setup/IP-Router/VRRP/VRRP-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.8.21.3 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.

**SNMP ID:** 2.8.21.3

**Telnet path:** Setup/IP-Router/VRRP

**Possible values:**

- 0 to 999 minutes

**Default:** 30 min.

### 2.8.21.4 Advert.-Interval

The advertising interval shows how many seconds until a virtual router is propagated again. All routers in virtual router system must be configured with the same value.

**SNMP ID:** 2.8.21.4

**Telnet path:** Setup/IP-Router/VRRP

**Possible values:**

- 0 to 999 seconds

**Default:** 1 seconds

### 2.8.21.5 Internal-Services

The Internal services checkbox controls how the router should behave when it is addressed via a virtual router address. In the default 'on' position, the router reacts to DNS and NETBIOS services exactly as if it had been addressed via its actual address. This only occurs when the device itself is the master of the virtual router. The 'off' setting results in RFC-compliant behavior, i.e. relevant packets are rejected.

**SNMP ID:** 2.8.21.5

**Telnet path:** Setup/IP-Router/VRRP

**Possible values:**

- Yes
- Off

**Default:** Yes

## 2.8.22 WAN-Tag-Creation

WAN tag creation defines the source for the assignment of interface tags. Besides assignment via the firewall or direct assignment via the tag table, the interface tag can also be selected based on the effective routing table (static routing entries plus routes learned via RIP). The tag selected from this routing table is is for the route that matches both the remote site and the associated network. If the effective routing table contains more than one entry for a remote site with the same network, the smallest tag is used.

**SNMP ID:** 2.8.22

**Telnet path:** /Setup/IP-Router

**Possible values:**

- Manual: With this setting, the interface tags are determined solely by an entry in the tag table. The routing table has no significance in the assignment of interfaces tags.
- Auto: With this setting, the interface tags are determined initially by an entry in the Tag table. If no matching entry is located there, the tag is determined based on the routing table.

**Default:** Manual:

**Note:** The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

### 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.

**SNMP ID:** 2.8.23

**Telnet path:** /Setup/IP-Router

## 2.8.23.1 Peer

Name of the remote site whose packets are to be given interface tags when received.

**SNMP ID:** 2.8.23.1

**Telnet path:** /Setup/IP-Router/Tag-Table

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

**Special values:** 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.

### 2.8.23.2 Rtg-Tag

This interface tag is assigned to the inbound packets of the remote site.

**SNMP ID:** 2.8.23.2

**Telnet path:** /Setup/IP-Router/Tag-Table

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.8.23.3

**Telnet path:** /Setup/IP-Router/Tag-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.8.23.4 End-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.

**SNMP ID:** 2.8.23.4

**Telnet path:** /Setup/IP-Router/Tag-Table

**Possible values:**

- Valid IP address

**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.

**Telnet path:**

**Setup** > **IP-Router** > **Tag-Table**

**Possible values:**

Valid IPv6 address

**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**.

**Telnet path:**

**Setup** > **IP-Router** > **Tag-Table**

**Possible values:**

Valid IPv6 address

**Default:**

0.0.0.0

### 2.8.23.7 NBNS-Default

Using this entry you configure the address that the remote station is assigned as its NBNS server.

If the specified value is `0.0.0.0`, your device assigns the NBNS server that is configured in the setup menu under **TCP-IP/NBNS-Default**. If `0.0.0.0` is also entered there, your device assigns itself as the NBNS server, if NetBIOS proxy is enabled.

**Telnet path:**

**Setup** > **IP-Router** > **Tag-Table**

**Possible values:**

Valid IPv6 address

**Default:**

0.0.0.0

### 2.8.23.8 NBNS-Backup

Using this entry you configure the address that the remote station is assigned as an alternate NBNS 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/NBNS-Backup**.

**Telnet path:**

**Setup** > **IP-Router** > **Tag-Table**

**Possible values:**

Valid IPv6 address

**Default:**

0.0.0.0

## 2.9 SNMP

This menu contains the configuration of SNMP.

**SNMP ID:** 2.9

**Telnet 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.

**SNMP ID:** 2.9.1

**Telnet path:** /Setup/SNMP

**Possible values:**

- Yes
- No

**Default:** No

## 2.9.2 IP-Traps

You can enter SNMP managers here.

**SNMP ID:** 2.9.2

**Telnet path:** /Setup/SNMP

## 2.9.2.1 Trap-IP

Enter the IP address of the computer where an SNMP manager is installed.

**SNMP ID:** 2.9.2.1

**Telnet path:** /Setup/SNMP/IP-Traps

**Possible values:**

- Valid IP address

**Default:** Blank

### 2.9.2.3 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.

**SNMP ID:** 2.9.2.3

**Telnet path:** /Setup/SNMP/IP-Traps

**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

**Default:** Blank

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

### 2.9.2.4 Version

Indicates SNMP version that should be used for the traps sent to this receiver.

**SNMP ID:** 2.9.2.4

**Telnet path:** /Setup/SNMP/IP-Traps

**Possible values:**

- SNMPv1
- SNMPv2

**Default:** SNMPv2

### 2.9.2.5 Port

Enter the port of the computer where an SNMP manager is installed.

**Telnet path:**
**Setup** > **SNMP** > **IP-Traps**

**Possible values:**
Max. 5 characters from `0123456789`
0 … 65535

**Default:**
*empty*

## 2.9.3 Administrator

Name of the device administrator. For display purposes only.

**SNMP ID:** 2.9.3

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

## 2.9.4 Location

Location information for this device. For display purposes only.

**SNMP ID:** 2.9.4

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.9.5

**Telnet path:** /Setup/SNMP

**Possible values:**

- <IP-Address|*>:<Port|*> <MAC-Address|*> <W>

**Default:** Blank

**Special values:** <W> at the end of the command is necessary if registration is to be effected over a wireless LAN connection.

**Note:** 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.

## 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.

**SNMP ID:** 2.9.6

**Telnet path:** /Setup/SNMP

**Possible values:**

- <IP-Address|*>:<Port|*>

**Default:** Blank

## 2.9.7 Monitor-Table

The monitor table shows all SNMP agents registered with the device.

**SNMP ID:** 2.9.7

**Telnet path:** /Setup/SNMP

### 2.9.7.1 IP-Address

IP address of the remote station from where an SNMP agent accesses the device.

**SNMP ID:** 2.9.7.1

**Telnet path:** /Setup/SNMP/Monitor-Table

**Possible values:**

- Valid IP address

### 2.9.7.2 Port

Port used by the remote device to access the local device with an SNMP agent.

**SNMP ID:** 2.9.7.2

**Telnet path:** /Setup/SNMP/Monitor-Table

### 2.9.7.3 Timeout

Timeout in minutes until the remote device is removed from the monitor table.

**SNMP ID:** 2.9.7.3

**Telnet path:** /Setup/SNMP/Monitor-Table

### 2.9.7.4 MAC-Address

MAC address of the remote station from where an SNMP agent accesses the device.

**SNMP ID:** 2.9.7.4

**Telnet path:** /Setup/SNMP/Monitor-Table

### 2.9.7.5 Peer

Name of the remote station from where an SNMP agent accesses the device.

**SNMP ID:** 2.9.7.5

**Telnet path:** /Setup/SNMP/Monitor-Table

**Possible values:**

- Select from the list of defined peers.

## 2.9.7.6 Loopback-Addr.

Loopback address of the remote station from where an SNMP agent accesses the device.

**SNMP ID:** 2.9.7.6

**Telnet path:** /Setup/SNMP/Monitor-Table

**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

## 2.9.7.7 VLAN-ID

ID of the VLAN used by the remote device to access the local device with an SNMP agent.

**SNMP ID:** 2.9.7.7

**Telnet path:** /Setup/SNMP/Monitor-Table

## 2.9.7.8 LAN-Ifc

LAN Ifc used by the remote device to access the local device with an SNMP agent.

**SNMP ID:** 2.9.7.8

**Telnet path:** /Setup/SNMP/Monitor-Table

### 2.9.7.9 Ethernet-Port

Ethernet port used by the remote device to access the local device with an SNMP agent.

**SNMP ID:** 2.9.7.9

**Telnet path:** /Setup/SNMP/Monitor-Table

### 2.9.10 Password-Required-for-SNMP-Read-Access

This setting specifies whether a password is required to read SNMP messages with an SNMP agent (e.g. LANmonitor).

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**No**

This setting allows information about the state of the device, current connections, reports, etc., to be read out publicly via SNMP ('public' ready-only community enabled).

**Yes**

This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device ('public' ready-only community disabled). Authorization can be conducted either with the administrator-account access credentials or an access account created for the custom SNMP community.

**Default:**

No

### 2.9.11 Comment-1

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.11

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

### 2.9.12 Comment-2

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.12

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

### 2.9.13 Comment-3

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.13

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

### 2.9.14 Comment-4

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.14

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 characters

**Default:** Blank

## 2.9.15 Read-Only-Community

This parameter specifies an individual SNMP community for read access. Either specify a master password or a username:password pair. Leave the field blank if you do not wish to operate any other read-only community except for 'public' (assuming the latter is enabled).

**Note:** Disabling the community 'public' has no effect on accessing with the community created here. An individual SNMP read-only community always has an alternative access key, which is not tied to an administrator account.

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

No direct dependency on other values. However, **Read-Only-Community** under **Setup** > **SNMP** > **Read-Only Communities** does add additional read-only communities to the parameters defined here.

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

**Default:**

*empty*

## 2.9.16 Comment-5

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.16

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 alphanumerical characters

**Default:** Blank

## 2.9.17 Comment-6

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.17

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 alphanumerical characters

**Default:** Blank

## 2.9.17 Comment-7

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.17

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 alphanumerical characters

**Default:** Blank

## 2.9.17 Comment-8

Comment on this device. For display purposes only.

**SNMP ID:** 2.9.17

**Telnet path:** /Setup/SNMP

**Possible values:**

- Max. 255 alphanumerical characters

**Default:** Blank

## 2.9.20 Full host MIB

Please select whether a full host MIB is used for the device.

**SNMP ID:** 2.9.20

**Telnet path:** /Setup/SNMP/Full-Host-MIB

**Possible values**:

- No

▶ Yes

**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.

**Telnet path:**
**Setup** > **SNMP**

**Possible values:**
0 … 65535

**Default:**
161

## 2.9.22 Read-Only-Communities

In this table, you define further write-protected communities for SNMP access.

**Telnet path:**
**Setup** > **SNMP**

## 2.9.22.1 Read-Only-Community

This parameter specifies an additional individual SNMP community for read access. Either specify a master password or a username:password pair.

**Note:** Disabling the community 'public' has no effect on accessing with the community created here. An individual SNMP read-only community always has an alternative access key, which is not tied to an administrator account.

**Telnet path:**

**Setup** > **SNMP** > **Read-Only-Communities**

**Possible values:**

No direct dependency on other values. However, this parameter does supplement the **Read-Only-Community** under **Setup** > **SNMP** with additional read-only communities.

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

**Default:**

*empty*

## 2.9.23 Public-Comment-1

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

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

**Default:**

*empty*

## 2.9.24 Public-Comment-2

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

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

**Default:**

*empty*

## 2.9.25 Public-Comment-3

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

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

**Default:**

*empty*

## 2.9.26 Public-Comment-4

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

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

**Default:**

*empty*

# 2.10 DHCP

This menu contains the DHCP settings.

**SNMP ID:** 2.10

**Telnet 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.

**SNMP ID:** 2.10.6

**Telnet path:** Setup/DHCP

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.10.7

**Telnet path:** Setup/DHCP

**Possible values:**

- Max. 10 characters

**Default:** 500

## 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.

**SNMP ID:** 2.10.8

**Telnet path:** Setup/DHCP

## 2.10.8.1 IP-Address

IP address used by the client.

**SNMP ID:** 2.10.8.1

**Telnet path:** Setup/DHCP/DHCP-Table

**Possible values:**

- Valid IP address

## 2.10.8.2 MAC-Address

The client's MAC address.

**SNMP ID:** 2.10.8.2

**Telnet path:** Setup/DHCP/DHCP-Table

## 2.10.8.3 Timeout

Lease for the address assignment in minutes.

**SNMP ID:** 2.10.8.3

**Telnet path:** Setup/DHCP/DHCP-Table

## 2.10.8.4 Hostname

Name of the client, if it was possible to determine this.

**SNMP ID:** 2.10.8.4

**Telnet path:** Setup/DHCP/DHCP-Table

### 2.10.8.5 Type

The 'Type' field indicates how the address was assigned. This field may contain the following 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.

Unknown: 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.

**SNMP ID:** 2.10.8.5

**Telnet path:** Setup/DHCP/DHCP-Table

### 2.10.8.7 Ethernet-Port

Physical interface connecting the client to the device.

**SNMP ID:** 2.10.8.7

**Telnet path:** Setup/DHCP/DHCP-Table

### 2.10.8.8 VLAN-ID

The VLAN ID used by the client.

**SNMP ID:** 2.10.8.8

**Telnet path:** Setup/DHCP/DHCP-Table

### 2.10.8.9 Network name

Name of the IP network where the client is located.

**SNMP ID:** 2.10.8.9

**Telnet path:** Setup/DHCP/DHCP-Table

## 2.10.8.10 LAN-Ifc

The LAN interface that this entry refers to.

**SNMP ID:** 2.10.8.10

**Telnet path:** /Setup/DHCP/DHCP-Table/LAN-Ifc

## 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.

**Telnet 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.

**SNMP ID:** 2.10.9

**Telnet 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.

**SNMP ID:** 2.10.9.1

**Telnet path:** Setup/DHCP/Hosts

**Possible values:**

- Valid MAC address

**Default:** 000000000000

### 2.10.9.2 IP-Address

Enter the client IP address that is to be assigned to the client.

**SNMP ID:** 2.10.9.2

**Telnet path:** Setup/DHCP/Hosts

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.10.9.3 Hostname

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.

**SNMP ID:** 2.10.9.3

**Telnet path:** Setup/DHCP/Hosts

**Possible values:**

- Max. 30 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.10.9.4

**Telnet path:** Setup/DHCP/Hosts

**Possible values:**

- Max. 16 characters

**Default:** Blank

**Note:** You must enter the server providing the boot image and the name of the file on the server in the boot image table.

### 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.

**SNMP ID:** 2.10.9.5

**Telnet path:** Setup/DHCP/Hosts

**Possible values:**

- Max. 16 characters

**Default:** Blank

**Special values:** Blank: 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.

**Note:** 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.

## 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.

**SNMP ID:** 2.10.10

**Telnet 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.

**SNMP ID:** 2.10.10.1

**Telnet path:** Setup/DHCP/Alias-List

**Possible values:**

- Max. 16 characters

**Default:** Blank

### 2.10.10.2 Image file

Enter the name of the file on the server containing the boot image.

**SNMP ID:** 2.10.10.2

**Telnet path:** Setup/DHCP/Alias-List

**Possible values:**

- Max. 60 characters

**Default:** Blank

### 2.10.10.3 Image server

Enter the IP address of the server that provides the boot image.

**SNMP ID:** 2.10.10.3

**Telnet path:** Setup/DHCP/Alias-List

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.10.18 Ports

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

**SNMP ID:** 2.10.18

**Telnet path:** Setup/DHCP

## 2.10.18.2 Port

Select the logical interface for which the DHCP server should be enabled or disabled.

**SNMP ID:** 2.10.18.2

**Telnet 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 Enable DHCP

Enables or disables the DHCP server for the selected logical interface.

**SNMP ID:** 2.10.18.3

**Telnet path:** Setup/DHCP/Ports

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.10.19 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.

**SNMP ID:** 2.10.19

**Telnet path:** Setup/DHCP

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.10.20

**Telnet path:** Setup/DHCP/Network-list

## 2.10.20.1 Network name

The name of the network which the DHCP server settings apply to.

**SNMP ID:** 2.10.20.1

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 2.10.20.2 Start-Adress-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).

**SNMP ID:** 2.10.20.2

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.10.20.3 Ende-Adress-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).

**SNMP ID:** 2.10.20.3

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 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.

**SNMP ID:** 2.10.20.4

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 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.

**SNMP ID:** 2.10.20.5

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0 (broadcast address is determined automatically).

**Note:** 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.

## 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.

**SNMP ID:** 2.10.20.6

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.10.20.7 DNS-Default

IP address of the DNS name server that the requesting workstation should use.

**SNMP ID:** 2.10.20.7

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

▶ Valid IP address

**Default:** 0.0.0.0

**Note:** 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.

## 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

**SNMP ID:** 2.10.20.8

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

▶ Valid IP address

**Default:** 0.0.0.0

**Note:** 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.

## 2.10.20.9 NBNS-Default

IP address of the NBNS name server that the requesting workstation should use.

**SNMP ID:** 2.10.20.9

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

▶ Valid IP address

**Default:** 0.0.0.0

## 2.10.20.10 NBNS-Backup

IP address of the backup NBNS name server. The workstation will use this NBNS server if the first NBNS name server fails

**SNMP ID:** 2.10.20.10

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.10.20.11

**Telnet 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.
- Automatic: 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 requests': 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-Mode': 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.

**Default:** No

**Note:** 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.

## 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.

**SNMP ID:** 2.10.20.12

**Telnet 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.

**SNMP ID:** 2.10.20.13

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.10.20.14

**Telnet path:** Setup/DHCP/Network-list

**Possible values:**

- Yes
- No

**Default:** No

## 2.10.20.15 Adaption

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
- Network mask
- Broadcast address
- DNS server
- NBNS server
- Server ID

This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

**SNMP ID:** 2.10.20.15

**Telnet 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.

**SNMP ID:** 2.10.20.16

**Telnet 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

**Note:** 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.

## 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.

**SNMP ID:** 2.10.20.17

**Telnet path:** /Setup/DHCP/Network-list/2nd-Master-Server

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.10.20.18

**Telnet path:** /Setup/DHCP/Network-list/2nd-Master-Server

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.10.20.19

**Telnet path:** /Setup/DHCP/Network-list/2nd-Master-Server

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.10.21 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.

**SNMP ID:** 2.10.21

**Telnet path:** Setup/DHCP

## 2.10.21.1 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.

**SNMP ID:** 2.10.21.1

**Telnet path:** Setup/DHCP/Additional-Options

**Possible values:** Max. 3 characters

**Default:** Blank

**Note:** 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).

## 2.10.21.2 Network name

Name of the IP network where this DHCP option is to be used.

**SNMP ID:** 2.10.21.2

**Telnet path:** Setup/DHCP/Additional-Options

**Possible values:**

- Select from the list of defined IP networks.

**Default:** Blank

**Special values:** Blank: If no network name is specified the DHCP option defined in this entry will be used in all IP networks.

## 2.10.21.3 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`.

**Note:** The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

**Telnet path:**

**Setup** > **DHCP** > **Additional-Options**

**Possible values:**

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

**Default:**

*empty*

## 2.10.21.4 Type

Entry type.

**SNMP ID:** 2.10.21.4

**Telnet path:** Setup/DHCP/Additional-Options

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 timeout 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.

**Possible values:**

- String
- Integer8
- Integer16
- Integer32
- IP address

**Default:** String

**Note:** You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

## 2.10.22 Vendor-Class-Identifier

The vendor class ID (DHCP option 60) shows the type of device. The vendor class ID is always transmitted.

**Telnet path:**

**Setup** > **DHCP** > **Vendor-Class-Identifier**

**Possible values:**

Max. 63 characters

**Default:**

Blank

# 2.11 Config

Contains the general configuration settings.

**SNMP ID:** 2.11

**Telnet path:** /Setup

## 2.11.3 Password-Required-for-SNMP-Read-Access

If this option is activated and no password has been set, you will always be requested to set a password when you log in to the device.

**SNMP ID:** 2.11.3

**Telnet path:** Setup/Config

**Possible values:**

- Yes
- No

**Default:** No

## 2.11.4 Maximum connections

The maximum number of simultaneous configuration connections to this device.

**SNMP ID:** 2.11.4

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 0

**Special values:** 0 switches the limit off.

## 2.11.5 Config-Aging-Minutes

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

**SNMP ID:** 2.11.5

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 15

## 2.11.6 Language

Terminal mode is available in English or German. Devices are set with English as the default console language.

**SNMP ID:** 2.11.6

**Telnet path:** Setup/Config

**Possible values:**

- Deutsch
- English

**Default:** English

**Note:** 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.

## 2.11.7 Login-Error

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 are allowed before the device is locked.

**SNMP ID:** 2.11.7

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.11.8

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 45

**Special values:** 0 switches the lock off.

## 2.11.10 Display-Contrast

This item allows you to set the contrast for the display of the device.

**SNMP ID:** 2.11.10

**Telnet path:** /Setup/Config/Display-Contrast

**Possible values:**

- K1 (low contrast) to K8 (high contrast).

**Default:** K4

### 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.

**Note:** 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!

**Telnet path:**

**Setup** > **Config**

**Possible values:**

No

Yes

**Default:**

No

### 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.

**SNMP ID:** 2.11.15

**Telnet path:** Setup/Config

### 2.11.15.1 Ifc.

The interface that this entry refers to.

**SNMP ID:** 2.11.15.1

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** 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 (Simple Network Management Protocol). This protocol is required, for example, for configuring the device using the LANmonitor application.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** Default setting for the WAN interface.

**Default:**

Yes
No

## 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** 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.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** Default setting for the WAN interface.

**Default:**

Yes
No

## 2.11.15.10 Config Sync

Indicates whether a config sync is possible (restricted) via this interface.

**Telnet path:**

**Setup** > **Config** > **Access-Table**

**Possible values:**

**VPN**

Access is only possible via VPN.

**Note:** VPN-capable devices only.

**Yes**

Access is generally possible.

**Note:** By default via all interfaces except WAN.

**Read**

Access is read only.

**No**

Access is not possible.

**Note:** Default setting for the WAN interface.

**Default:**

Yes
No

## 2.11.16 Screen height

Specifies the maximum height of the screen in lines. Entering 0 here causes the device to determine optimum screen height automatically when you log in.

**SNMP ID:** 2.11.16

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 24

**Special values:** 0

## 2.11.17 Prompt

This value sets the prompt on the command line.

**SNMP ID:** 2.11.17

**Telnet path:** Setup/Config

**Possible values:**

- Max. 31 characters with the following variables:
- %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

**Default:** Blank

## 2.11.18 LED-Test

Activates the test mode for the LEDs to test LED function in different colors.

**SNMP ID:** 2.11.18

**Telnet 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.

**SNMP ID:** 2.11.20

**Telnet path:** Setup/Config

## 2.11.20.1 Index

Index for this entry.

**SNMP ID:** 2.11.20.1

**Telnet path:** /Setup/Config/Cron-Table

## 2.11.20.2 Minute

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

**SNMP ID:** 2.11.20.2

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- Max. 50 characters

**Default:** Blank

## 2.11.20.3 Hour

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

**SNMP ID:** 2.11.20.3

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- Max. 50 characters

**Default:** Blank

## 2.11.20.4 DayOfWeek

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

**SNMP ID:** 2.11.20.4

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- 0: Sunday
- 1: Monday
- 2: Tuesday
- 3: Wednesday
- 4: Thursday
- 5: Friday
- 6: Saturday

**Default:** Blank

## 2.11.20.5 Day

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

**SNMP ID:** 2.11.20.5

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- Max. 50 characters

**Default:** Blank

## 2.11.20.6 Month

The value defines the point in time when a command is to be executed. With no value entered, it is not included in the controlling. A comma-separated list of values can be entered, or alternatively a range of minimum and maximum values.

**SNMP ID:** 2.11.20.6

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- 0: Sunday
- 1: Monday
- 2: Tuesday
- 3: Wednesday
- 4: Thursday
- 5: Friday
- 6: Saturday

**Default:** Blank

## 2.11.20.7 Command

The command to be executed or a comma-separated list of commands. Any command-line function can be executed.

**SNMP ID:** 2.11.20.7

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- Max. 100 characters

**Default:** Blank

## 2.11.20.8 Base

The time base field determines whether time control is based on real time or on the device's operating time.

**SNMP ID:** 2.11.20.8

**Telnet 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.

**SNMP ID:** 2.11.20.9

**Telnet 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.

**SNMP ID:** 2.11.20.10

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.11.20.11

**Telnet path:** /Setup/Config/Cron-Table

**Possible values:**

- 0 to 65535 seconds

**Default:** 0

**Special values:** When set to zero, the CRON job is executed at precisely the defined time.

**Note:** Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.

## 2.11.20.12 Comment

This parameter is used to leave a comment about the entry in the CRON table.

**Telnet 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.

**SNMP ID:** 2.11.21

**Telnet 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.

**SNMP ID:** 2.11.21.1

**Telnet path:** Setup/Config/Admins

**Possible values:**

- Max. 16 characters

**Default:** Blank

**Note:** 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 WEB-config 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).

## 2.11.21.2 Password

Password for this entry.

**SNMP ID:** 2.11.21.2

**Telnet path:** Setup/Config/Admins

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 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.

**Telnet 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 link 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.
- 0x00001000: The user can run the Public-Spot User management Wizard.

**Default:**

Blank

## 2.11.21.4 Operating

Activates or deactivates the function

**SNMP ID:** 2.11.21.4

**Telnet 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:

- LAN

- Wireless LAN (WLAN)

- WAN (e.g. , 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.

**SNMP ID:** 2.11.21.5

**Telnet path:** Setup/Config/Admins

**Possible values:**

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

**Default:** Blank

## 2.11.23 Telnet-Port

This port is used for unencrypted configuration connections via Telnet.

**SNMP ID:** 2.11.23

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 23

### 2.11.25 SSH-Port

This port is used for configuration connections via SSH.

**SNMP ID:** 2.11.25

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 22

### 2.11.26 SSH-Authentication-Methods

Here you specify the authentication method to be used for SSH.

**SNMP ID:** 2.11.26

**Telnet path:** Setup/Config

## 2.11.26.1 Ifc.

The authentication methods permitted for SSH access can be set separately for LAN, WAN and WLAN.

**SNMP ID:** 2.11.26.1

**Telnet path:** /Setup/Config/SSH-Authentication-Methods

**Possible values:**

- LAN
- WAN
- WLAN

## 2.11.26.2 Methods

The SSH protocol generally allows two different authentication mechanisms: Username and password, using a public key, or interactively via the keyboard.

**SNMP ID:** 2.11.26.2

**Telnet path:** /Setup/Config/SSH-Authentication-Methods

**Possible values:**

- Public-Key: Only allows authentication with a digital certificate.
- Keyboard-interactive: Only allows authentication via the keyboard.
- Password: Only allows authentication with a password.
- Password+Keyboard-Interactive: Allows authentication with password or interactively via the keyboard.
- Password+Public-Key: Allows authentication using password or using digital certificate.
- Keyboard-Interactive+Public Key: Only allows authentication via the keyboard or via digital certificate.
- All: Allows authentication using any method.

**Default:** All

## 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.

**SNMP ID:** 2.11.27

**Telnet path:** /Setup/Config/Predef.-Admins

## 2.11.27.1 Name

Enter the name of the predefined administrator account here.

**SNMP ID:** 2.11.27.1

**Telnet path:** Setup/Config/Predef.-Admins/Name

**Possible Telnet values:**

- Maximum 16 characters

**Default:** Blank

## 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.

**Telnet 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.

**Telnet 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

MAC algorithms are used to check the integrity of messages. Select one or more of the available algorithms.

**Telnet 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

**Default:**

hmac-md5-96,hmac-md5,hmac-sha1-96,hmac-sha1,hmac-sha2-256-96, hmac-sha2-256,hmac-sha2-512-96,hmac-sha2-512

## 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.

**Telnet 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**

**Default:**

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256

## 2.11.28.4 Host key algorithms

The host key algorithms are used to authenticate hosts. Select one or more of the available algorithms.

**Telnet path:**

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

**Possible values:**

**ssh-rsa**
**ssh-dss**
**ecdsa-sha2**
**ssh-ed25519**

**Default:**

ssh-rsa
ssh-dss

## 2.11.28.5 Min-Hostkey-Length

This parameter defines the minimum length of your host keys.

**Telnet path:**

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

**Possible values:**

Max. 5 numbers

**Default:**

512

## 2.11.28.6 Max-Hostkey-Length

This parameter defines the maximum length of your host keys.

**Telnet path:**

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

**Possible values:**

Max. 5 numbers

**Default:**

8192

## 2.11.28.7 DH-Groups

The Diffie-Hellman groups are used for the key exchange. Select one or more of the available groups.

**Telnet path:**

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

**Possible values:**

Group-1

Group-5

Group-14

Group-15

Group-16

**Default:**

Group-1,Gruppe-5,Gruppe-14

## 2.11.28.8 Compression

With this setting, you enable or disable compression of data packets for connections using SSH.

**Telnet 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).

**Note:** 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`.

**Telnet 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.

**Telnet path:**

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

### 2.11.28.10.1 Operating

You enable or disable the SFTP server with this setting.

**Telnet 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 HiLCOS SSH server sends keepalives to keep a connection open.

**Telnet path:**

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

**Possible values:**

0 … 99999 Seconds

**Special values:**

**0**

This value disables the function.

**Default:**

60

## 2.11.29 Telnet-SSL

The parameters for Telnet-SSL connections are specified here.

**Telnet path:**

**Setup** > **Config**

## 2.11.29.2 Versions

This bitmask specifies which versions of the protocol are allowed.

**Telnet path:**

**Setup** > **Config** > **Telnet-SSL**

**Possible values:**

**SSLv3**

**TLSv1**
**TLSv1.1**
**TLSv1.2**

**Default:**
TLSv1

## 2.11.29.3 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

**Telnet path:**
**Setup** > **Config** > **Telnet-SSL**

**Possible values:**

**RSA**
**DHE**
**ECDHE**

**Default:**
RSA
DHE
ECDHE

## 2.11.29.4 Crypro algorithms

This bitmask specifies which cryptographic algorithms are allowed.

**Telnet path:**
**Setup** > **Config** > **Telnet-SSL**

**Possible values:**

**RC4-40**

**RC4-56**
**RC4-128**
**DES40**
**DES**
**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.

**Telnet 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.

**Telnet 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.

**Telnet 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

## 2.11.29.10 PORT

This port is used for encrypted configuration connections via telnet.

**Telnet path:**
**Setup** > **Config** > **Telnet-SSL**

**Possible values:**
0 … 65535

**Default:**
992

## 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.

**SNMP ID:** 2.11.32

**Telnet 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 (default setting): 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.

**Note:** Further information about the different boot configurations are to be found in the reference manual.

**Default:** reset or boot

**Note:** After a reset, the access point returns to managed mode, in which case the configuration cannot be directly accessed via the WLAN interface!

**Note:** After resetting, the device starts completely unconfigured and all settings are lost. If possible be sure to backup the current device configuration before resetting.

**Note:** 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 HiLCOS reference manual.

### 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.

**SNMP ID:** 2.11.33

**Telnet path:** Setup/Config

**Possible values:**

- Max. 10 characters

**Default:** 1

### 2.11.35 Monitor trace

This menu contains the settings for monitor tracing.

**SNMP ID:** 2.11.35

**Telnet path:** Setup/Config

## 2.11.35.1 Tracemask1

This parameter is for support purposes only.

**SNMP ID:** 2.11.35.1

**Telnet path:** /Setup/Config/Monitortrace

### 2.11.35.2 Tracemask2

This parameter is for support purposes only.

**SNMP ID:** 2.11.35.2

**Telnet path:** /Setup/Config/Monitortrace

## 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.

**Telnet path:**Setup/Config//License-Expiry-Email

**Possible values:**

- Valid e-mail address

**Default:** Blank

## 2.11.40 Crash-Message

Here you specify the message that appears in the bootlog when the device crashes.

**SNMP ID:** 2.11.40

**Telnet path:** /Setup/Config/Crash-Message

**Possible values:**

- Maximum 32 alphanumerical characters

**Default:** HiLCOS-Watchdog

## 2.11.41 Admin-Gender

Enter the sex of the Admin.

**SNMP ID:** 2.11.41

**Telnet path:** /Setup/Config/Admin-Gender

**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.

**SNMP ID:** 2.11.42

**Telnet path:** /Setup/Config/Assert-Action

**Possible values:**

- log_only
- reboot

**Default:** log_only

**Note:** 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.

### 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.

**SNMP ID:** 2.11.43

**Telnet path:** Setup/Config

## 2.11.43.1 Key

Name of function key.

**SNMP ID:** 2.11.43.1

**Telnet path:** Setup\Config\Function-Keys

**Possible values:**

- Selection from function keys F1 to F12.

**Default:** F1

## 2.11.43.2 Mapping

Description of the command/shortcut to be run on calling the function key in the command line.

**SNMP ID:** 2.11.43.2

**Telnet path:** Setup\Config\Function-Keys

**Possible values:**

- All commands/shortcuts possible in the command line

**Default:** Blank

**Special values:** The caret symbol ^ is used to represent special control commands with ASCII values below 32.^a

^A stands for Ctrl-A (ASCII 1)

^Z stands for Ctrl-Z (ASCII 26)

^[ stands for Escape (ASCII 27)

^M stands for 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.

**Note:** 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.

**Note:** This value exists only in the SNMP chain.

**Telnet path:**
**Setup** > **Config** > **Config-Date**

**Possible values:**
Valid configuration date

### 2.11.50 LL2M

The menu contains the settings for LANCOM layer-2 management.

**SNMP ID:** 2.11.50

**Telnet path:** Setup/Config

## 2.11.50.1 Enabled

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.

**SNMP ID:** 2.11.50.1

**Telnet 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.

**SNMP ID:** 2.11.50.2

**Telnet path:** /Setup/Config/LL2M

**Possible values:**

- 0 to 4294967295

**Default:** 0

**Special values:** 0 disables the time limit. The LL2M server stays permanently enabled in this state.

## 2.11.51 Sync

In this directory, you configure the automatic configuration synchronization.

**Telnet path:**
**Setup** > **Config**

## 2.11.51.1 Operating

Activates or deactivates the automatic configuration synchronization.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync**

### 2.11.51.2.1 Name

Enter an identifier for this entry.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **New Cluster**

#### *2.11.51.2.2.1 Idx.*

Index for this entry in the list.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **New Cluster**

#### *2.11.51.2.3.1 Idx.*

Index for this entry in the list.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** The display is updated after you save the entry.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **New Cluster**

##### *2.11.51.2.4.1 Idx.*

Index for this entry in the list.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** The display is updated after you save the entry.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync**

#### 2.11.51.3.1 Port

Specify the port to be used by the device to receive incoming configuration changes.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **Renew-Snapshot**

#### 2.11.51.4.1 Modification limit

Enter the modification limit here.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **Renew-Snapshot**

## 2.11.51.5 Local configuration

In this directory you specify the number of applied and detected modifications.

**Telnet path:**

**Setup** > **Config** > **Sync** > **Local Config**

### 2.11.51.5.1 Detected modifications

Specify the number of detected modifications.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Sync** > **Local Config**

**Possible values:**

Max. 10 characters from `0123456789`

## 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.

Meaned values for CPU load are available in the following time intervals:

**SNMP ID:** 2.11.60

**Telnet path:** Setup/Config

**Possible values:**

T1s (arithmetic mean)

T5s (arithmetic mean)

T60s (moving average)

T300s (moving average)

**Default:** T60s

## 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.

**Note:** To document sporadic errors, disable this option with the entry `0`.

**Telnet 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.

## 2.11.73 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.

**Telnet 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.

- **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.

**Note:** 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**.

**Note:** 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.

**Telnet path:**

**Setup** > **Config**

**Possible values:**

Internal

Radius

TACACS+

**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.

**Telnet path:**

**Setup** > **Config**

## 2.11.81.1 Server

This table contains the settings for the RADIUS server.

**Telnet path:**

**Setup** > **Config** > **Radius**

#### 2.11.81.1.1 Name

Enter a name for the RADIUS server.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 2.11.81.1.2 Server

Enter the IPv4 address of the RADIUS server here.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

Max. 64 characters

**Default:**

Blank

#### 2.11.81.1.3 Port

Specify here the port used by the RADIUS server to communicate with the device.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

Max. 5 characters

**Default:**

1812

#### 2.11.81.1.4 Protocol

Specify here the protocol used by the RADIUS server to communicate with the device.

**Telnet 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.

**Telnet 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.

**Note:** 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.

**Default:**

Blank

### 2.11.81.1.6 Secret

Enter the password for accessing the RADIUS server and repeat it in the second input field.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

Max. 64 characters

**Default:**

Blank

#### 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.

**Note:** The backup server requires an additional entry in the Server table.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 2.11.81.1.8 Category

Set the category for which the RADIUS server applies.

You can select No, one or both categories.

**Telnet 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.

**Telnet path:**

**Setup** > **Config** > **Radius** > **Server**

**Possible values:**

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

**Default:**

*empty*

## 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 |

**Note:** 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.

**Telnet path:**

**Setup** > **Config** > **Radius**

**Possible values:**

**Vendor specific**
**Mapped**
**Shell privilege**

**Default:**

Vendor specific

## 2.11.81.3 Account IP

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.

**Telnet path:**

**Setup** > **Config** > **Radius**

**Possible values:**

No

Yes

**Default:**

No

## 2.11.90 LED mode

You set the operating mode of the device LEDs here.

**Notice:** The "LED-Test" function is available despite the LEDs being disabled.

**Telnet 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.

**Note:** If you change this value and save it within the previously set time, you should restart the timer.

**Telnet path:**

**Setup** > **Config**

**Possible values:**

Max. 4 characters `0123456789`

**Default:**

300

## 2.12 WLAN

This menu contains the settings for wireless LAN networks

**SNMP ID:** 2.12

**Telnet 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).

**SNMP ID:** 2.12.3

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 3 numbers

**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.

**SNMP ID:** 2.12.8

**Telnet path:** /Setup/WLAN

**Possible values:**

- Filter out data from listed stations, transfer all other
- transfer data from the listed stations, authenticate all other 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.

**SNMP ID:** 2.12.12

**Telnet 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.

**SNMP ID:** 2.12.13

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 10 numbers

**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.

**SNMP ID:** 2.12.14

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 10 numbers

**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.

**SNMP ID:** 2.12.26

**Telnet path:** /Setup/WLAN

**Possible values:**

- Yes
- No

**Default:** Yes

**Note:** 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.

## 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.

**SNMP ID:** 2.12.27

**Telnet 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

**SNMP ID:** 2.12.29

**Telnet path:** /Setup/WLAN

## 2.12.29.2 Auth.-Port

Port for communication with the RADIUS server during authentication

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Valid port specification

**Default:** 1812

## 2.12.29.3 Key

Password used to access the RADIUS server

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.12.29.5 Backup-Auth.-Port

Port for communication with the backup RADIUS server during authentication

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Valid port specification

**Default:** 1812

## 2.12.29.6 Backup-Key

Password used to access the backup RADIUS server

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 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.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Max. 10 numeric characters ranging from 0 to 4294967295 (2^32-1)

**Default:** 15

**Note:** Recently cached MAC address entries can be viewed in the table '1.3.48 RADIUS-Cache '.

## 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.

**Telnet 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.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- Max. 10 numeric characters ranging from 0 – 4294967295 (2^32-1)

**Default:** 0

## 2.12.29.10 Provide-Server-Database

Activate this option if the MAC address list is provided by a RADIUS server.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- No
- Yes

**Default**: Yes

## 2.12.29.11 Loopback-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.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**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

**Default:** Blank

**Note:** If there is an interface named "DMZ", then its address is used.

## 2.12.29.12 Backup-Loopback-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.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check

**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
- LBO ... LBF for the 16 loopback addresses
- Any valid IP address

**Default:** Blank

## 2.12.29.13 Protocol

Protocol for communication between the RADIUS server and the clients.

**SNMP ID:** 2.12.29.13

**Telnet path:** /Setup/WLAN/RADIUS-Access-Check

**Possible values:**

- RADSEC
- RADIUS

**Default:** RADIUS

## 2.12.29.14 Backup-Protocol

Protocol for communication between the backup RADIUS server and the clients.

**Telnet path:**/Setup/WLAN/RADIUS-Access-Check/Backup-Protocol

**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.

**Telnet path:**

**Setup** > **WLAN** > **RADIUS-Access-Check**

**Possible values:**

MAC address(es) of registered clients using spaces as separators

## 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).

**Note:** The RADIUS client automatically detects which address type is involved.

**Note:** 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.

**Note:** 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.

**Telnet 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).

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet 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`.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN** > **RADIUS-Access-Check**

**Possible values:**

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

**Default:**

*empty*

## 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.

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

Select from the list of countries

**Note:** If you select the value **unknown**, the device allows only those parameters that are approved worldwide!

**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.

**SNMP ID:** 2.12.38

**Telnet path:** /Setup/WLAN

**Possible values:**

- On
- Off

**Default:** On

**Note:** As of HiLCOS version 8.00, this switch activates a similar treatment for IPv6 neighbor solicitations.

## 2.12.41 Mail-Address

Information about events in the WLAN is sent to this e-mail address.

**SNMP ID:** 2.12.41

**Telnet path:** /Setup/WLAN

**Possible values:**

- Valid e-mail address

**Default:** Blank

**Note:** An SMTP account must be set up to make use of the e-mail function.

## 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.

**SNMP ID:** 2.12.44

**Telnet 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.

**SNMP ID:** 2.12.45

**Telnet path:** /Setup/WLAN

## 2.12.45.8 Interim-Update-Period

This value sets the time interval in seconds after which the device sends an interim update to the accounting server.

**SNMP ID:** 2.12.45.8

**Telnet path:** /Setup/WLAN/RADIUS-Accounting

**Possible values:**

- Max. 10 numeric characters in the range 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.

**SNMP ID:** 2.12.45.9

**Telnet path:** /Setup/WLAN/RADIUS-Accounting

**Possible values:**

- Max. 4 numeric characters in the range 0 – 9999
- 0 deactivates this function.

**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.

**Telnet path:**/Setup/WLAN/RADIUS-Accounting/Restart-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.

**Telnet 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.

**Telnet 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

**Telnet 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.

**Telnet 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

**Note:** 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

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Note:** You also need to set the general values for retry and timeout in the RADIUS section.

**Telnet 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`.

**Telnet path:**

**Setup** > **WLAN** > **RADIUS-Accounting** > **Servers**

**Possible values:**

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

**Default:**

*empty*

## 2.12.46 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.

**SNMP ID:** 2.12.46

**Telnet path:** /Setup/WLAN

**Possible values:**

- On
- Off

**Default:** Off

**Note:** Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

**Note:** Indoor operation may only be activated if the base station and all other stations are operated within an enclosed space.

## 2.12.47 Idle-Timeout

This is the time in seconds during which the access point cannot receive any packets after a client is disconnected.

**SNMP ID:** 2.12.47

**Telnet path:** /Setup/WLAN/Idle-Timeout

**Possible Telnet values:**

- Max. 10 numerical characters

**Default:** 3600 seconds

### 2.12.50 Signal averaging

This menu contains the settings for signal averaging.

**SNMP ID:** 2.12.50

**Telnet path:** /Setup/WLAN

**Note:** 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.

## 2.12.50.1 Method

Method for signal averaging.

**SNMP ID:** 2.12.50.1

**Telnet path:** /Setup/WLAN/Signal-Averaging

**Possible values:**

- Standard
- Filtered

**Default:** Standard

**Note:** 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.

## 2.12.50.2 Standard-Parameters

This menu contains the configuration of the default parameters for signal averaging.

**SNMP ID:** 2.12.50.2

**Telnet path:** /Setup/WLAN/Signal-Averaging

**Note:** 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.

#### 2.12.50.2.1 Factor

Factor for the signal averaging.

**Telnet path:**/Setup/WLAN/Signal-Averaging/Standard-Parameters

**Possible values:**

- Max. 3 numerical characters

**Default:** 4

**Note:** 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.

### 2.12.51 Rate-Adaption

This menu contains the settings for the rate-adaption algorithm.

**SNMP ID:**

2.12.51

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN** > **Rate-Adaptation**

**Possible values:**

Minimum

RSSI-dependent

**Default:**

Minimum

## 2.12.51.3 Minstrel averaging factor

The averaging factor used for recalculating the net rates for each bit rate according to the Minstrel method.

**Telnet path:**

**Setup** > **WLAN** > **Rate-Adaptation**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **WLAN** > **Rate-Adaptation**

**Possible values:**

0 to 99

**Default:**

0

### 2.12.51.5 Method

Sets the method of rate adaptation.

**Telnet path:**

**Setup** > **WLAN** > **Raten-Adaptation** > **Method**

**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.

**SNMP ID:** 2.12.60

**Telnet path:** /Setup/WLAN

**Possible values:**

- Select from the list of ARF networks defined in the device
- Maximum 16 alphanumerical characters

**Default:** Blank

**Special values:** Blank: 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.

**Telnet path:**

**Setup** > **WLAN** > **VLAN-groupkey-mapping**

### 2.12.70.1 Network

Contains the name of a WLAN network registered in the device.

**Telnet path:**

**Setup** > **WLAN** > **VLAN-groupkey-mapping**

### 2.12.70.2 VLAN-Id

Contains the VLAN ID assigned to the logical WLAN network.

**Telnet path:**

**Setup** > **WLAN** > **VLAN-groupkey-mapping**

**Possible values:**

1 to 4094

**Default:**

1

### 2.12.70.3 Group key index

The table contains the group key index.

**Telnet path:**

**Setup** > **WLAN** > **VLAN-groupkey-mapping**

**Possible values:**

1 to 3

## 2.12.80 Dual-Roaming

Here is where you manage the roaming behavior of devices with multiple WLAN modules.

**Telnet path:**

**Setup** > **WLAN** > **Dual-Roaming**

### 2.12.80.1 Group

Determines whether all WLAN modules participate in dual-roaming.

**Telnet path:**

**Setup** > **WLAN** > **Dual-Roaming**

**Possible values:**

Off

WLAN-1 + WLAN-2

**Default:**

Off

### 2.12.80.2 Lockout-Period-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.

**Telnet path:**

**Setup** > **WLAN** > **Dual-Roaming**

**Possible values:**

0 to 4294967295

**Default:**

100

### 2.12.85 PMK-Caching

Manage PMK-caching here.

**Telnet path:**

**Setup** > **WLAN** > **PMK-Caching**

### 2.12.85.1 Default-Lifetime

Specifies the duration in seconds that the WLAN client stores the negotiated PMK.

**Note:** 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.

**Telnet path:**

**Setup** > **WLAN** > **PMK-Caching**

**Possible values:**

0 to 4294967295

**Default:**

0

**Special values:**

0: The negotiated PMK expires immediately.

## 2.12.86 Paket-Capture

This menu contains the settings for packet capturing.

**Telnet 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*.

**Telnet 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 HiLCOS 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 priority 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 Band-Steering

This is where you specify the 'WLAN band steering' settings of the WLAN clients registered at the access point.

**Telnet path:**

**Setup** > **WLAN**

## 2.12.87.1 Enabled

This option enables 'band steering' in the access point.

**Telnet path:**

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

**Possible values:**

Yes

No

**Default:**

No

## 2.12.87.3 Preferred-Band

Set here the preferred frequency band to which the access point steers the WLAN client.

**Telnet path:**

**Setup** > **WLAN** > **Band-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.

**Note:** 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.

**Telnet path:**

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

**Possible values:**

Max. 10 characters

From 0 to 9

**Special values:**

0: The visible probe requests are deemed invalid immediately.

**Default:**

120

### 2.12.87.5 Initial block time

If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, 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.

**Note:** 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.

**Telnet path:**

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

**Possible values:**

Max. 10 characters from `0123456789`

**Special values:**

**0**

This value disables the delay.

**Default:**

10

### 2.12.88 Error-Monitoring

This is where you determine the 'Error-Monitoring' settings. Using the error monitoring the user may define, how many errors of dedicated error types are allowed during a give time range, before the chosen recovery action will be triggered. The recovery action will be executed in order to get the device back to a normal operation status.

**Telnet path:**

**Setup** > **WLAN**

## 2.12.88.1 Errors

Select the type or error, which should trigger the selected recovery action.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

Bus-Errors

NIC-Errors

AGC-Calibrate-Failures

Stuck-Interrupts

**Default:**

AGC-Calibrate-Failures

Stuck-Interrupts

## 2.12.88.2 Time

Select the time interval for the error monitoring. If the defined limit for an active error type is reached during this time, the selected recovery action will be triggered.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

0 to 4294967295 seconds

**Default:**

60 seconds

## 2.12.88.3 Bus-Error-Count

Select the amount of bus errors, which should trigger the selected recovery action.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

0 to 9

**Default:**

5

## 2.12.88.4 Boot-Type

Select the appropriate recovery action, which should be executed once the defined limit for an active error type is reached.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

Warm-Boot

Cold-Boot

**Default:**

Warm-Boot

## 2.12.88.5 NIC-Error-Count

Select the amount of nic errors, which should trigger the selected recovery action.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

0 to 9

**Default:**

5

## 2.12.88.6 AGC-Cal-Failure-Count

Select the amount of AGC calculation errors, which should trigger the selected recovery action.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

0 to 9

**Default:**

5

## 2.12.88.7 Stuck-Interrupt-Count

Select the amount of stuck interrupts, which should trigger the selected recovery action.

**Telnet path:**

**Setup** > **WLAN** > **Error-Monitoring**

**Possible values:**

0 to 9

**Default:**

5

## 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.

**Telnet path:**

**Setup** > **WLAN**

## 2.12.89.1 MAC address pattern

Enter the MAC address of a station.

**Note:** It is possible to use wildcards.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Important:** The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

**Note:** This field has no significance for networks secured by WEP.

**Telnet path:**

**Setup** > **WLAN** > **Access rules**

**Possible values:**

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

## 2.12.89.5 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.

**Note:** 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".

**Telnet 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

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.

**Note:** 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".

**Telnet 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.

**Telnet 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.

**Note:** The use of wildcards makes it possible to allow access to multiple SSIDs.

**Telnet 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.

**SNMP ID:** 2.12.100

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 10 numbers

**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).

**SNMP ID:** 2.12.101

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 10 numbers

**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.

**SNMP ID:** 2.12.103

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 12 hexadecimal characters

**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.

**SNMP ID:** 2.12.105

**Telnet path:** /Setup/WLAN

**Possible values:**

- Max. 10 numbers

**Default:** 20

**Special values:** 0: Deactivates this function.

**Note:** Please note that deactivating the thermal recalibration cycle for these cards means that they cannot react to changes in temperature.

### 2.12.109 Noise-Offsets

This table is used to define the correction factors which adjust the displayed signal values.

**SNMP ID:** 2.12.109

**Telnet path:** /Setup/WLAN

## 2.12.109.1 Band

The noise-offset value is applied to the frequency band selected here.

**SNMP ID:** 2.12.109.1

**Telnet path:** /Setup/WLAN/Noise-Offsets

**Possible values:**

- Choose from the frequency bands supported by the device, e.g. 2.4 GHz or 5 GHz.

**Default:** 2.4 GHz

## 2.12.109.2 Channel

The noise-offset value is applied to the channel selected here.

**SNMP ID:** 2.12.109.2

**Telnet path:** /Setup/WLAN/Noise-Offsets

**Possible values:**

- Max. 5 numerical characters

**Default:** Blank

## 2.12.109.3 Interface

The noise-offset value is applied to the WLAN interface selected here.

**SNMP ID:** 2.12.109.3

**Telnet path:** /Setup/WLAN/Noise-Offsets

**Possible values:**

- Depend on the hardware capabilities, e.g. WLAN-1 or WLAN-2

**Default:** WLAN-1

## 2.12.109.4 Value

This numeric value is added to the current noise value.

**SNMP ID:** 2.12.109.4

**Telnet path:** /Setup/WLAN/Noise-Offsets

**Possible values:**

- Max. 3 numeric characters in the range 0 – 127

**Default:** 0

## 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.

**SNMP ID:** 2.12.110

**Telnet 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

**Default:** 255

## 2.12.111 Noise-Immunity

The settings for noise-immunity (Adaptive Noise Immunity - ANI) can be adjusted here.

**SNMP ID:** 2.12.111

**Telnet path:** /Setup/WLAN/Noise-Immunity

**Note:** 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.

## 2.12.111.1 Noise-Immunity

This item sets the threshold value to be used for noise immunity.

**Telnet path:**/Setup/WLAN/Noise-Immunity/Noise-Immunity-Level

**Possible values:**

- Numerical characters from 0 to 255

**Default:** 255

**Note:** 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.

## 2.12.111.2 OFDM-Weak-Signal-Detection

This item sets the threshold value to be used for detecting weak OFDM signals.

**Telnet path:**/Setup/WLAN/Noise-Immunity/OFDM-Weak-Signal-Detection

**Possible values:**

- Numerical characters from 0 to 255

**Default:** 255

**Note:** 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.

## 2.12.111.3 CCK-Weak-Signal-Detection-Threshold

This item sets the threshold value to be used for detecting weak CCK signals.

**Telnet path:**/Setup/WLAN/Noise-Immunity/CCK-Weak-Signal-Detection-Threshold

**Possible values**

- Numerical characters from 0 to 255

**Default:** 255

**Note:** 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.

## 2.12.111.4 Fir-Step-Level

This item sets the value to be used for the fir step.

**Telnet path:**/Setup/WLAN/Noise-Immunity/Fir-Step

**Possible values:**

- Numerical characters from 0 to 255

**Default:** 255

**Note:** 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.

## 2.12.111.5 Spurious-Immunity-Level

This item sets the threshold value to be used for spurious immunity.

**Telnet path:**/Setup/WLAN/Noise-Immunity/Spurious-Immunity-Level

**Possible values**

- Numerical characters from 0 to 255

**Default:** 255

**Note:** 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.

## 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.

**Telnet path:**

**Setup** > **WLAN** > **Noise-Immunity**

**Possible values:**

0 to 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

**SNMP ID:** 2.12.114

**Telnet path:** /Setup/WLAN/Aggregate-Retry-Limit

**Possible values:**

- 0 to 255

**Default:** 255

**Note:** The absolute value set under 'Hard-Retries' for transmission attempts remains unaffected by the setting here.

## 2.12.115 Omit-Global-Crypto-Sequence-Check

This is where you set the value for the crypto sequence check.

**SNMP ID:** 2.12.115

**Telnet path:** /Setup/WLAN

**Possible values:**

- Auto
- Yes
- No

**Default:** Auto

**Special values:** Auto: HiLCOS 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.

## 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).

**SNMP ID:** 2.12.116

**Telnet path:** /Setup/WLAN

**Possible values:**

- One or more values from Management, Control, Data, EAPOL, 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.

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

0 to 4294967295

**Default:**

0

## 2.12.118WPA-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.

**Telnet path:**

**Setup** > **WLAN** > **WPA-Handshake-Timeout-Override-ms**

**Possible values:**

0 to 4294967295

**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.

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

0 to 4294967295

**Default:**

40

## 2.12.121 HT-Fairness

HT fairness is used for mixed operation with devices that do support 802.11n and those that do not, in order to ensure approximately equal access to broadcast facilities for both types of clients. The devices uses a different strategy when selecting which packets are to be transmitted.

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

Yes

No

**Default:**

Yes

## 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

**Telnet 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

**Telnet path:**
**Setup** > **WLAN**

**Possible values:**
**Normal**
All normal data packets
**NULL**
All empty data packets
**Other**
All other data packets

## 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.

**Telnet 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.

**Important:** Please not that activating this option constitutes a breach of ETSI regulations because no approval has been granted for HiLCOS.

### Telnet 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.

### Telnet 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.

**Telnet 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 750).

**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.

**Important:** 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.

**Important:** This parameter is required exclusively for development tests and is not relevant for normal operations. Never change this default setting!

**Telnet 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.

**Telnet path:**
**Setup** > **WLAN** > **DFS**

**Possible values:**

**No**
**Yes**

**Default:**

Yes

## 2.12.130.6 Trace ignored pulses

This parameter specifies whether HiLCOS conducting the DFS pulse trace reports radar pulses that are reported by the WLAN hardware but are rejected by the software as being invalid.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Important:** Changing these default values may cause the device to operate in violation of the standard ETSI EN 301 893 version 1.3.

**Telnet path:**

**Setup** > **WLAN** > **DFS** > **Radar-Pattern-Thresholds**

**Possible values:**

0 … 4294967295

**Default:**

depending on the selected radar pattern

## 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.

**Telnet path:**

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

## 2.12.248.9 IDS-Operational

Enable or disable Wireless IDS here.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

E-mail sending for each event

**Default:**

10

## 2.12.248.43 Intruder-Identification

Enable or disable Wireless IDS intruder identification here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

**Possible values:**

**No**

Wireless IDS intruder identification is disabled

**Yes**

Wireless IDS intruder identification is enabled

**Default:**

No

## 2.12.248.44 Timeout-Intruder-Activity

Here you specify the time following an attack after which the status of the attacker is set to inactive.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

**Possible values:**

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

**Default:**

60

## 2.12.248.45 Store-Intruder-DHCP-Requests

Enable or disable the storage of intruder DHCP requests here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

**Possible values:**

**No**

The storage of intruder DHCP requests is disabled

**Yes**

The storage of intruder DHCP requests is enabled

**Default:**

No

## 2.12.248.50 Signatures

Here you define the threshold values/intervals that provide the ability to help detect different kinds of potential intrusion attacks.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

### 2.12.248.50.1 AssociateReqFlood

An attacker continually sends association frames to the AP. This overloads the AP's association table.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.1.1 CounterLimit*

Set the threshold value for associate request frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

**Possible values:**

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

**Default:**

250

#### *2.12.248.50.1.2 CounterInterval*

Here you specify the period of time in which the associate request frames are counted. If the device counts more associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **AssociateReqFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.2 ReassociateReqFlood

Attacks using re-associate request frames

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.2.1 CounterLimit*

Set the threshold value for re-associate request frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

**Possible values:**

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

**Default:**

250

### *2.12.248.50.2.2 CounterInterval*

Here you specify the period of time in which the re-associate request frames are counted. If the device counts more re-associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **ReassociateReqFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.3 AuthenticateReqFlood

An attacker continually sends authentication frames to the AP. This overloads the AP's authentication table.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.3.1 CounterLimit*

Set the threshold value for authenticate request frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

**Possible values:**

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

**Default:**

250

### *2.12.248.50.3.2 CounterInterval*

Here you specify the period of time in which the authenticate request frames are counted. If the device counts more authenticate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **AuthenticateReqFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.4 EAPOLStart

If an AP receives an EAPOL-Start frame, it starts the identification process and allocates resources internally to the new client. An attacker can generate a lot of EAPOL-Start frames to exhaust the access point interval resource and overload the RADIUS server.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.4.1 CounterLimit*

Set the threshold value for the EAPOL-Start frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

**Possible values:**

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

**Default:**

250

#### *2.12.248.50.4.2 CounterInterval*

Specify the period of time in which the EAPOL-Start frames are counted here. If the device counts more EAPOL-Start frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **EAPOLStart**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.5 ProbeBroadcast

An attacker continually sends probe requests to the network. Basically, probe requests are frames used by clients to ask: "Is there a WLAN here?" Probe responses are sent by the APs to reply "Yes, there's a WLAN here with SSID". This is a mechanism for discovering WLAN services in WLAN networks. If the attacker sends sufficient probe requests, the AP will be overloaded with these probe requests and the wireless medium will be flooded with probe responses.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.5.1 CounterLimit*

Set the threshold value for the broadcast probe frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

**Possible values:**

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

**Default:**

500

#### *2.12.248.50.5.2 CounterInterval*

Specify the period of time in which the broadcast probe frames are counted here. If the device counts more broadcast probe frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **ProbeBroadcast**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.6 DisassociateBroadcast

An attacker sends a spoof disassociation frame with broadcast destination address to the network. Clients that receive the frame will be diassociated and re-association to the AP is required. Management frames that include disassociation are not protected and are sent in clear text. The described attack is thus easy to carry out. Data communication between the AP and the clients is not possible until the clients reassociate.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.6.1 CounterLimit*

Set the threshold value for broadcast disassociate frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

**Possible values:**

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

**Default:**

2

### *2.12.248.50.6.2 CounterInterval*

Here you specify the period of time in which the broadcast disassociate frames are counted. If the device counts more broadcast disassociate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateBroadcast**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

1

### 2.12.248.50.7 DeauthenticateBroadcast

An attacker sends a spoof deauthentication frame with broadcast destination address to the network. Clients that receive the frame will be deauthenticated and re-authentication to the AP is required. Management frames that include deauthentication are not protected and are sent in clear text. The described attack is thus easy to carry out. Data communication between the AP and the clients is not possible until the clients reauthenticate.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.7.1 CounterLimit*

Set the threshold value for broadcast deauthenticate frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

**Possible values:**

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

**Default:**

2

#### *2.12.248.50.7.2 CounterInterval*

Here you specify the period of time in which the broadcast deauthenticate frames are counted. If the device counts more broadcast deauthenticate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateBroadcast**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

1

### 2.12.248.50.8 DisassociateReqFlood

An attacker spoofs disassociation frames in order to log off a client from the AP. All clients affected then attempt to reassociate with the AP. No data communication is possible until the clients reassociate.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.8.1 CounterLimit*

Set the threshold value for dis-associate request frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

**Possible values:**

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

**Default:**

250

### *2.12.248.50.8.2 CounterInterval*

Here you specify the period of time in which the dis-associate request frames are counted. If the device counts more dis-associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DisassociateReqFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.9 BlockAckOutOfWindow

**Block-Ack DoS attack**

An attacker spoofs the MAC address of the client and is able to conduct the following attacks:

1. During the setup phase of a block-ACK session, the attacker sends an ADDBA frame with a manipulated starting sequence number to the AP. In this way, the attacker causes the AP to discard legitimate frames.
2. The attacker sends manipulated A-MPDU frames, which overload of the re-ordering buffer on the AP.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.9.1 CounterLimit*

Here you set the threshold value on the out-of-window frames that are received during a block-ack session.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

**Possible values:**

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

**Default:**

200

### *2.12.248.50.9.2 CounterInterval*

Here you specify the time interval for counting the out-of-window frames. If the device counts more out-of-window frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckOutOfWindow**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.12.248.50.10 BlockAckAfterDelBA

**Block-Ack DoS attack**

An attacker spoofs the MAC address of the client and is able to conduct the following attacks: The attacker stops the block-ACK session with a fake DELBA frame from the client to the AP, resulting in the loss of buffered frames on the AP. An attack with manipulated DELBA frames can also reduce throughput, because the client is forced to re-establish the block-ACK session.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.10.1 CounterLimit*

Here you set the threshold value for block-ACK-session frames that arrive after receiving the DELBA frame.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

**Possible values:**

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

**Default:**

100

### *2.12.248.50.10.2 CounterInterval*

Here you specify the time interval for counting the Block-Ack-session frames. If the device counts more Block-Ack-session frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **BlockAckAfterDelBA**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

## 2.12.248.50.11 NullDataFlood

**Null-data DoS attack**

If a client is inactive for a long period, the AP is unable to decide whether the client is switched off or merely outside of the radio cell. One consequence could be for the AP to deauthenticate the client. To prevent accidental deauthentication, the client sends null-data frames to the AP after a period of inactivity in order to keep the session alive. The AP then acknowledges the receipt of the null-data frame. An attacker can take advantage of this scenario in the following way:

The attacker sends large numbers of null-data frames to the AP. Because the AP is forced to acknowledge the receipt of every individual null-data frame, the bandwidth on the radio channel is reduced to such an extent that legitimate client requests are discarded.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.11.1 CounterLimit*

Here you set the threshold value for received null-data frames.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

**Possible values:**

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

**Default:**

500

### *2.12.248.50.11.2 CounterInterval*

Here you specify the time interval for counting the null-data frames. If the device counts more null-data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.12.248.50.12 NullDataPSBufferOverflow

**Null-data PS attack**

A client can use null-data frames to inform the AP that it is entering into the sleep mode. In this case, the AP buffers the packets that arrive for the client in sleep mode, and it informs the client that packets are buffered at the AP by using the TIM field of beacon frames. Upon receipt of beacon frames that have the corresponding TIM bit set, the client uses a PS-poll frame to request the packets from the buffer of the AP. An attacker can take advantage of this scenario in the following way:

The attacker spoofs the MAC address of the client and sends the AP a fake notification about going into sleep mode. The AP now buffers the incoming packets for the client and these packets will be dropped after a certain timeout. This continues as long as the client does not send a PS-poll frame. Because in reality the client is not in the sleep mode at all, it will not send a PS-poll frame to request buffered packets from the AP. This leads to the loss of the packets addressed to the client.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.12.1 CounterLimit*

Here you set the threshold value for the data frames that were deleted due to a buffer overflow.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

**Possible values:**

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

**Default:**

200

### *2.12.248.50.12.2 CounterInterval*

Here you specify the time interval for counting the deleted data frames. If the device counts more data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **NullDataPSBufferOverflow**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

## 2.12.248.50.13 PSPollTIMInterval

**PS-poll attack**

The attacker spoofs the MAC address of the client in sleep mode and sends fake PS-poll frames to the AP in order to request the buffered packets. The attacker now retrieves the packets that were intended for the client.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.13.1 CounterLimit*

Here you set the threshold value for the PS-poll frames that are received after the listen interval difference is exceeded.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

**Possible values:**

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

**Default:**

100

### *2.12.248.50.13.2 CounterInterval*

Here you specify the time interval for counting the PS-poll frames. The program triggers an alarm if, within this time interval, the device counts any additional PS-poll frames arriving after the "PSPollTIMIntervalDiff" is exceeded and that exceed the limit set for the "PSPollTIMIntervalDiffCounter".

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

#### *2.12.248.50.13.3 Interval-Diff*

Here you specify when, at the earliest, the client is allowed to send a PS-poll frame to the AP before the specified TIM interval expires.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **PSPollTIMInterval**

**Possible values:**

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

**Default:**

5

### 2.12.248.50.14 SMPSMultiStream

The use of multiple antennas on the same transmission channel enhances data throughput and improves the signal coverage. The operation of multiple antennas is energy intensive, so in times of low data throughput a client switches into static spatial multiplexing power save mode (SM power save mode) and just one antenna remains active. The client uses SM-power-save-action frames to inform the AP about a change into SM power save mode or the end of the SM power save mode. An attacker can take advantage of this scenario in the following way: The attacker spoofs the MAC address of a client in static SM power save mode with just one active antenna and uses a fake SM-power-save-action frame to inform the AP that it is ending its static SM power save mode. The AP then communicates with the client via multiple spatial streams, which the client is not able to receive using only one active antenna.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

### *2.12.248.50.14.1 CounterLimit*

Here you specify the threshold value for the number of data frames the client transmits using multiple spatial streams after the client has switched into the static SM power save mode.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMultiStream**

**Possible values:**

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

**Default:**

100

### *2.12.248.50.14.2 CounterInterval*

Here you specify the time interval for counting the data frames the client transmits using multiple spatial streams. If the device counts more data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSMultiStream**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.12.248.50.15 DeauthenticateReqFlood

An attacker continually sends spoof deauthentication frames from the AP to a client. Similarly, the client will be deauthenticated and data communication will be terminated until the client reassociates to the AP.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.15.1 CounterLimit*

Set the threshold value for deauthenticate frames here.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

**Possible values:**

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

**Default:**

250

#### *2.12.248.50.15.2 CounterInterval*

Here you specify the period of time in which the deauthenticate frames are counted. If the device counts more deauthenticate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **DeauthenticateReqFlood**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.12.248.50.18 SMPSSingleStream

The use of multiple antennas on the same transmission channel enhances data throughput and improves the signal coverage. The operation of multiple antennas is energy intensive, so in times of low data throughput a client switches into static spatial multiplexing power save mode (SM power save mode) and just one antenna remains active. The client uses SM-power-save-action frames to inform the AP about a change into SM power save mode or the end of the SM power save mode. An attacker can take advantage of this scenario in the following way: The attacker spoofs the MAC address of a client with multiple active antennas and uses a fake SM-power-save-action frame to inform the AP that it is going into the static SM power save mode. The AP then communicates with the client over a single spatial stream, which significantly reduces the throughput.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures**

#### *2.12.248.50.18.1 CounterLimit*

Here you specify the threshold value for the number of failed data frame transmissions from the AP using multiple spatial streams to the client after the client has disabled the static SM power save mode.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSSingleStream**

**Possible values:**

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

**Default:**

100

### *2.12.248.50.18.2 CounterInterval*

Here you specify the time interval for counting the failed data frame transmissions from the AP using multiple spatial streams. If the device counts more failed data frame transmissions within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **Signatures** > **SMPSSingleStream**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

## 2.12.248.101 WIDS-White-List-Table

By entering certain stations into in a white list here, you exclude them from the intruder identification.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS**

### 2.12.248.101.1 Station-Id

Here you specify the station ID as the index of the table.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **WIDS-White-List-Table**

**Possible values:**

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

### 2.12.248.101.2 Station-MAC

Here you specify the MAC address of the station that is to be excluded from intruder identification.

**Telnet path:**

**Setup** > **WLAN** > **Wireless-IDS** > **WIDS-White-List-Table**

**Possible values:**

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

## 2.12.249 WLAN link status log

Use this item to make the settings for the WLAN link status log. The WLAN link status log enables you to capture and monitor information about the quality of the WLAN links.

**Telnet path:**

**Setup** > **WLAN**

## 2.12.249.10 Active

You activate or deactivate the WLAN link status log function here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

**Possible values:**

**No**

WLAN link status log function disabled

**Yes**

WLAN link status log function enabled

**Default:**

No

## 2.12.249.11 SNMP-Traps-Active

Here you enable or disable the transmission of SNMP traps by the WLAN link status log.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

**Possible values:**

**No**

SNMP trap transmission by the WLAN link status log disabled

**Yes**

SNMP trap transmission by the WLAN link status log enabled

**Default:**

No

## 2.12.249.12 Syslog-Active

Here you enable or disable the creation of syslog entries by the WLAN link status log.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

**Possible values:**

**No**

Creation of syslog entries by the WLAN link status log is disabled

**Yes**

Creation of syslog entries by the WLAN link status log is enabled

**Default:**

No

## 2.12.249.13 USB-Logging-Active

This is where you enable or disable the storage of information about the WLAN link status logs on the USB storage device ACA21 under the following file name: `WirelessWlanLinkStatusLogReports.txt`

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

**Possible values:**

**No**

Disables storage on the USB storage device ACA21

**Yes**

Enables storage on the USB storage device ACA21

**Default:**

No

## 2.12.249.14 Sampling-Interval

Here you set the time intervals at which information about the quality of WLAN links is written to the WLAN link status log. The time interval is derived from the added values for hours, days, and months.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

### 2.12.249.14.1 Months

Specify the time interval in months here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Sampling-Interval**

**Possible values:**

Max. 1 characters from `[0-9]`

**Default:**

1

### 2.12.249.14.2 Days

Specify the time interval in days here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Sampling-Interval**

**Possible values:**

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

**Default:**

0

### 2.12.249.14.3 Hours

Specify the time interval in hours here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Sampling-Interval**

**Possible values:**

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

**Default:**

10

## 2.12.249.15 Link-Age-Out-Time

Here you specify the time interval after which the monitoring of an inactive WLAN link is stopped. The time interval is derived from the added values for hours, days, and months.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log**

### 2.12.249.15.1 Months

Specify the time interval in months here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Link-Age-Out-Time**

**Possible values:**

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

**Default:**

2

### 2.12.249.15.2 Days

Specify the time interval in days here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Link-Age-Out-Time**

**Possible values:**

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

**Default:**

0

### 2.12.249.15.3 Hours

Specify the time interval in hours here.

**Telnet path:**

**Setup** > **WLAN** > **WLAN-Link-Status-Log** > **Link-Age-Out-Time**

**Possible values:**

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

**Default:**

20

## 2.12.250 Roaming-Statistics-Timeout

Here you specify the timeout value for an entry in the roaming statistics table. If an entry is not updated within the timeout period, the entry is deleted. Rebooting the device also resets the entries.

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

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

**Special values:**

**0**

None of the entries in the roaming statistics table are deleted.

**Default:**

86400

## 2.12.251 Prioritized-Channel-Scan

The prioritized channel scan function optimizes roaming by including previous roaming decisions. This is suitable for scenarios with recurring movements of the clients within the WLAN. The prioritized channel scan function selects

channels where potential roaming candidates are most likely to be found. This results in accelerated roaming, reduced handover times, and less packet loss.

**Telnet path:**

**Setup** > **WLAN**

## 2.12.251.1 Minimum-Roam-Count

Here you specify the minimum roam count for the roaming entries. Only when the minimum roam count has been reached is the prioritized channel scan function enabled. The minimum roam count helps to prevent premature channel prioritization.

**Telnet path:**

**Setup** > **WLAN** > **Prioritized-Channel-Scan**

**Possible values:**

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

**Default:**

2

## 2.12.251.2 Normal-Scan-Cycle-Period

Here you specify the number of scan cycles to perform before a regular, complete scan cycle takes place.

**Telnet path:**

**Setup** > **WLAN** > **Prioritized-Channel-Scan**

**Possible values:**

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

**Special values:**

**0**

No regular, complete scan cycle is performed but exclusively prioritized channel scans instead.

**1**

Regular, complete scan cycle is performed for all scan cycles.

**Default:**

4

## 2.14 Time

This menu contains the configuration of the device time settings.

**SNMP ID:** 2.14

**Telnet path:** /Setup

### 2.14.1 Fetch-Method

Select here if and how the device synchronizes its internal real-time clock.

**Telnet path:**

**Setup** > **Time**

**Possible values:**

None

NTP

**Default:**

NTP

### 2.14.2 Current-Time

Display of current time.

**SNMP ID:** 2.14.2

**Telnet path:** /Setup/Time

## 2.14.7 UTC-in-Seconds

This parameter is used by LANmonitor to read the time.

**Telnet path:**
**Setup** > **Time**

## 2.14.10 Timezone

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)

**SNMP ID:** 2.14.10

**Telnet path:** /Setup/Time

**Possible values:**

- 0
- +1
- +2
- +3
- +4
- +5
- +5:30
- +6
- +7
- +8
- +9
- +10
- +11
- +12
- +13
- +14
- -1
- -2
- -3
- -4

- -5
- -6
- -7
- -8
- -9
- -10
- -11
- -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.

**SNMP ID:** 2.14.11

**Telnet 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'.

**SNMP ID:** 2.14.12

**Telnet path:** /Setup/Time

### 2.14.12.1 Event

Defines the beginning and end of daylight saving time

**Telnet path:** /Setup/Time/DST-Clock-Changes

### 2.14.12.2 Index

First or last day of month for switching to daylight-saving time (summertime).

**Telnet 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.

**Telnet path:** /Setup/Time/DST-Clock-Changes

### 2.14.12.4 Month

The month in which the change is carried out.

**Telnet path:** /Setup/Time/DST-Clock-Changes

### 2.14.12.5 Hour

The hour at which the change is carried out.

**Telnet path:** /Setup/Time/DST-Clock-Changes

### 2.14.12.6 Minute

The minute at which the change is carried out.

**Telnet path:** /Setup/Time/DST-Clock-Changes

### 2.14.12.7 Time-type

Time standard, such as UTC (Coordinated Universal Time).

**Telnet 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.

**SNMP ID:** 2.14.13

**Telnet path:** /Setup/Time

### 2.14.15 Holidays

This table contains the holidays that have been defined.

**SNMP ID:** 2.14.15

**Telnet path:** /Setup/Time/Holidays

### 2.14.15.1 Index

This describes the position of the entry in the table.

**SNMP ID:** 2.14.15.1

**Telnet path:** /Setup/Time/Holidays/Index

**Possible values:**

- 0 to 9999

**Default:** Blank

### 2.14.15.2 Date

If you have created entries in the least-cost table or the timed control table that should apply on public holidays, enter the days here.

**SNMP ID:** 2.14.15.2

**Telnet path:** /Setup/Time/Holidays/Date

**Possible values:**

- Valid date

**Default:** Blank

### 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.

**SNMP ID:** 2.14.16

**Telnet path:** /Setup/Time

## 2.14.16.1 Name

Enter the name of the timeframe for referencing from the content-filter profile.

**SNMP ID:** 2.14.16.1

**Telnet path:** /Setup/Time/Timeframe

**Possible values:**

- Name of a timeframe
- Maximum 31 characters

**Default:** Blank

## 2.14.16.2 Start

Here you set the start time (time of day) when the selected profile becomes valid.

**SNMP ID:** 2.14.16.2

**Telnet path:** /Setup/Time/Timeframe

**Possible values:**

- Max. 5 characters
- Format HH:MM

**Default:** 00:00

### 2.14.16.3 Stop

Here you set the end time (time of day) when the selected profile becomes invalid.

**SNMP ID:** 2.14.16.3

**Telnet path:** /Setup/Time/Timeframe

**Possible values:**

- Max. 5 characters
- Format HH:MM

**Default:** 23:59

### 2.14.16.4 Weekdays

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

**SNMP ID:** 2.14.16.4

**Telnet path:** /Setup/Time/Timeframe

**Possible values:**

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday
- Public holiday

**Default:** Activated for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

# 2.15 LCR

This menu contains the configuration of the least-cost router.

**SNMP ID:** 2.15

**Telnet path:** /Setup

## 2.15.1 Router-Usage

A router is an intelligent network component; comparable with a post office, it uses the logical target address of a packet to determine which network component should transmit the packet next; it knows the overall topology of the network. If this option is activated, all connections made by the router are controlled by least-cost routing.

**SNMP ID:** 2.15.1

**Telnet path:** /Setup/LCR

**Possible values:**

- Yes
- No

**Default:** No

## 2.15.4 Time-List

In this table you can define the Call-by-Call numbers to be used for telephone calls depending on the time, day and area code.

**SNMP ID:** 2.15.4

**Telnet path:** /Setup/LCR

## 2.15.4.1 Index

Index for this entry in the table.

**SNMP ID:** 2.15.4.1

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Max. 10 characters

**Default:** 0

## 2.15.4.2 Prefix

Enter the prefix (e.g. area code) or the first few digits of a group of prefixes to which the entry will apply. If, for example, you enter 030 for Berlin, all calls with this prefix will be redirected as indicated here. Optionally you may wish to enter only 03 and then all calls to any place that begins with the prefix 03 will be redirected accordingly.

**SNMP ID:** 2.15.4.2

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Max. 10 characters

**Default:** Blank

## 2.15.4.3 Days

The days on which this entry should apply. You can create multiple entries for a given prefix, each applying to different periods or different days.

**SNMP ID:** 2.15.4.3

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday

- Saturday
- Sunday
- Public holiday

**Default:** Blank

## 2.15.4.4 Start

The start of the period during which this entry should apply.

**SNMP ID:** 2.15.4.4

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Max. 5 characters

**Default:** Blank

## 2.15.4.5 Stop

The end of the period during which this entry should apply.

**SNMP ID:** 2.15.4.5

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Max. 5 characters

**Default:** Blank

## 2.15.4.6 Number list

Enter here the prefix for the call-by-call provider to be used for calls matching this entry.

Multiple prefixes can be separated by semi-colons. If no connection can be established with the first prefix, the following prefixes will be tried in sequence.

Leave this field empty if calls that match this entry are not to be re-directed.

**SNMP ID:** 2.15.4.6

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Max. 29 characters

**Default:** Blank

### 2.15.4.7 Fallback

Automatic fallback: If no connection can be established on any of the supplied call-by-call numbers, the least-cost router will connect to your regular telephone service provider. Switch this option off if you do not want this to happen.

**SNMP ID:** 2.15.4.7

**Telnet path:** /Setup/LCR/Time-List

**Possible values:**

- Yes
- No

**Default:** No

## 2.16 NetBIOS

This menu contains the configuration of the NetBIOS.

**SNMP ID:** 2.16

**Telnet path:** /Setup

### 2.16.1 Operating

When this option is enabled, the device will also be able to forward NetBIOS packets directly to specific stations in remote networks. Without this option enabled, these packets often cause unnecessary connections, since the individual computers of NetBIOS-based networks (e.g. Microsoft Windows networks) continuously exchange status information.

**SNMP ID:** 2.16.1

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- Yes
- No

**Default:** No

## 2.16.2 Scope-ID

The device appends this string to the NetBIOS name for all TCP/IP connections using NetBIOS.

**SNMP ID:** 2.16.2

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.16.4 Peers

Enter the name for the remote stations to which NetBIOS is to be transmitted over IP. These remote sites also have to be entered into the IP routing table.

**SNMP ID:** 2.16.4

**Telnet path:** /Setup/NetBIOS

## 2.16.4.1 Name

Enter the name for the remote station here. This remote station must also be present in the routing table of the IP router.

**SNMP ID:** 2.16.4.1

**Telnet path:** /Setup/NetBIOS/Peers

**Possible values:**

- Max. 16 characters

**Default:** Blank

### 2.16.4.3 Type

Specify whether the remote station is a router or an individual workstation with a dial-up remote-access connection.

**SNMP ID:** 2.16.4.3

**Telnet path:** /Setup/NetBIOS/Peers

**Possible values:**

- Workstation
- Router

**Default:** Router

## 2.16.5 Group list

This list displays all NetBIOS groups.

**SNMP ID:** 2.16.5

**Telnet path:** /Setup/NetBIOS

### 2.16.5.1 Group/Domain

Name of the workgroup communicated by NetBIOS.

**SNMP ID:** 2.16.5.1

**Telnet path:** /Setup/NetBIOS/Group-List

### 2.16.5.2 Type

NetBIOS defines a certain amount of server types, and these are displayed by hexadecimal numbers. The most important of these types are:

- Standard-Workstation 00
- Win PopUp service 03
- RAS-Server 06
- Domain master browser or PDC 1B

- Master-Browser 1D
- NetDDE service 1F
- File or printer service 20
- RAS-Client 21
- Network monitor agent BE
- Network monitor utility BF

**SNMP ID:** 2.16.5.2

**Telnet path:** /Setup/NetBIOS/Group-List

### 2.16.5.3 IP-Address

The station's IP address.

**SNMP ID:** 2.16.5.3

**Telnet path:** /Setup/NetBIOS/Group-List

**Possible values:**

- Valid IP address

### 2.16.5.4 Peer

Name of the remote device that can be used to access this NetBIOS group.

**SNMP ID:** 2.16.5.4

**Telnet path:** /Setup/NetBIOS/Group-List

**Possible values:**

- Select from the list of defined peers.

### 2.16.5.5 Timeout

Period of validity (lease) of this entry in minutes.

**SNMP ID:** 2.16.5.5

**Telnet path:** /Setup/NetBIOS/Group-List

### 2.16.5.6 Flags

Flags as additional identifiers for the station or group.

**SNMP ID:** 2.16.5.6

**Telnet path:** /Setup/NetBIOS/Group-List

### 2.16.5.7 Network name

Name of the IP network where the client is located.

**SNMP ID:** 2.16.5.7

**Telnet path:** /Setup/NetBIOS/Group-List

### 2.16.5.8 Rtg-Tag

Routing tag for this entry.

**SNMP ID:** 2.16.5.8

**Telnet path:** /Setup/NetBIOS/Group-List

## 2.16.6 Host List

This list displays all NetBIOS hosts.

**SNMP ID:** 2.16.6

**Telnet path:** /Setup/NetBIOS

### 2.16.6.1 Name

Name of the station communicated by NetBIOS.

**SNMP ID:** 2.16.6.1

**Telnet path:** /Setup/NetBIOS/Host-List

### 2.16.6.2 Type

NetBIOS defines a certain amount of server types, and these are displayed by hexadecimal numbers. The most important of these types are:

- Standard-Workstation 00
- Win PopUp service 03
- RAS-Server 06
- Domain master browser or PDC 1B
- Master-Browser 1D
- NetDDE service 1F
- File or printer service 20
- RAS-Client 21
- Network monitor agent BE
- Network monitor utility BF

**SNMP ID:** 2.16.6.2

**Telnet path:** /Setup/NetBIOS/Host-List

### 2.16.6.3 IP-Address

The station's IP address.

**SNMP ID:** 2.16.6.3

**Telnet path:** /Setup/NetBIOS/Host-List

**Possible values:**

- Valid IP address

### 2.16.6.4 Peer

Name of the remote site that can be used to access this station.

**SNMP ID:** 2.16.6.4

**Telnet path:** /Setup/NetBIOS/Host-List

**Possible values:**

- Select from the list of defined peers.

### 2.16.6.5 Timeout

Period of validity (lease) of this entry in minutes.

**SNMP ID:** 2.16.6.5

**Telnet path:** /Setup/NetBIOS/Host-List

### 2.16.6.6 Flags

Flags as additional identifiers for the station or group.

**SNMP ID:** 2.16.6.6

**Telnet path:** /Setup/NetBIOS/Host-List

### 2.16.6.7 Network name

Name of the IP network where the client is located.

**SNMP ID:** 2.16.6.7

**Telnet path:** /Setup/NetBIOS/Host-List

### 2.16.6.8 Rtg-Tag

Routing tag for this entry.

**SNMP ID:** 2.16.6.8

**Telnet path:** /Setup/NetBIOS/Host-List

## 2.16.7 Server-List

This list displays all NetBIOS servers.

**SNMP ID:** 2.16.7

**Telnet path:** /Setup/NetBIOS

### 2.16.7.1 Host

Displays the host's NetBIOS name

**SNMP ID:** 2.16.7.1

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.2 Group/Domain

Displays the workgroup/domain where the NetBIOS host is located.

**SNMP ID:** 2.16.7.2

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.4 IP-Address

Displays the IP address of the NetBIOS host.

**SNMP ID:** 2.16.7.4

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.5 OS-Ver.

Displays the NetBIOS host's operating system.

**SNMP ID:** 2.16.7.5

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.6 SMB-Ver.

Displays the SMB version of the NetBIOS host.

**SNMP ID:** 2.16.7.6

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.7 Server-Type

Displays the NetBIOS host's server type.

**SNMP ID:** 2.16.7.7

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.8 Peer

Remote device over which the NetBIOS host can be reached.

**SNMP ID:** 2.16.7.8

**Telnet path:** /Setup/NetBIOS/Server-List

**Possible values:**

- Select from the list of defined peers.

### 2.16.7.9 Timeout

Displays the time in minutes until the NetBIOS information is updated.

**SNMP ID:** 2.16.7.9

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.10 Flags

Displays the NetBIOS flags detected for the NetBIOS host.

**SNMP ID:** 2.16.7.10

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.11 Network name

Displays the IP network where the NetBIOS host is located.

**SNMP ID:** 2.16.7.11

**Telnet path:** /Setup/NetBIOS/Server-List

### 2.16.7.12 Rtg-Tag

Routing tag for the connection to the NetBIOS host.

**SNMP ID:** 2.16.7.12

**Telnet path:** /Setup/NetBIOS/Server-List

## 2.16.8 Watchdogs

Some stations send watchdog packets from time to time to check whether other stations in the network can be reached. Watchdogs of this type can cause unnecessary connections to be established. Here you can specify whether the device should intercept watchdogs of this type and answer them itself to prevent these connections from being established.

**SNMP ID:** 2.16.8

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- Spoof
- Route

**Default:** Spoof

## 2.16.9 Update

The device has to exchange routing information with other NetBIOS routers from time to time. To avoid unnecessary connections being established, select when this should occur.

**SNMP ID:** 2.16.9

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- pBack
- Trig
- Time

**Default:** pBack

### 2.16.10 WAN-Update-Minutes

If you have specified that routing information should be exchanged at particular intervals, enter this interval here in minutes.

**SNMP ID:** 2.16.10

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- Max. 10 characters

**Default:** 60

### 2.16.11 Lease time

The maximum time in minutes for which NetBIOS names remain valid.

A host registers with the device with a NetBIOS name. When this period expires, then the host must re-register with its name.

**SNMP ID:** 2.16.11

**Telnet path:** /Setup/NetBIOS

**Possible values:**

- Max. 10 numerical characters

**Default:** 500

### 2.16.12 Networks

This table is used to adjust NetBIOS settings and to select the network that they apply to.

**SNMP ID:** 2.16.12

**Telnet path:** /Setup/NetBIOS

## 2.16.12.1 Network name

Select here the name of the network to which the settings are to apply.

**SNMP ID:** 2.16.12.1

**Telnet path:** /Setup/NetBIOS/Networks

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 2.16.12.2 Operating

Select here whether or not the NetBIOS proxy is to be used for the selected network.

**SNMP ID:** 2.16.12.2

**Telnet path:** /Setup/NetBIOS/Networks

**Possible values:**

- Yes
- No

**Default:** No

## 2.16.12.3 NT-Domain

Enter the name of the workgroup used by the computers in your network. If several workgroups exist within your network, entering one name is sufficient.

**SNMP ID:** 2.16.12.3

**Telnet path:** /Setup/NetBIOS/Networks

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 2.16.13 Browser-List

This table shows you an overview of the master browsers known to the NetBIOS proxy.

**Telnet path:**

**Setup** > **NetBIOS**

## 2.16.13.1 Browser

This entry shows the computer name (master browser).

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.2 Group/Domain

This entry shows the workgroups/domains.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.4 IP-Address

This entry shows the IP addresses.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.5 OS-Ver.

This entry shows the OS version.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.7 Server-Type

This entry shows the server type.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.8 Peer

This entry shows the name of the remote station.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.9 Timeout

This entry shows the number of timeouts.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.10 Flags

This entry shows the flags.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.11 Network name

This entry shows the network name.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

## 2.16.13.12 Rtg-Tag

This entry shows the routing tag used.

**Telnet path:**

**Setup** > **NetBIOS** > **Browser-List**

### 2.16.14 Support-Browsing

Windows uses the browser service or search service to discover the network environment. Since the browser service works with broadcasts, the network environment in routed networks is incomplete if no domains are used. Support of the search service closes this gap by propagating the master browser for each local workgroup to the remote side, or by using broadcasts in the LAN to propagate the master browsers located on the remote side. The list of master browsers known to the NetBIOS proxy can be viewed under /Status/TCP-IP/NetBIOS/Browser-List. Support of the search service only needs to be activated in workgroup networks. Domain networks operate without broadcasts, and the master browser is always the domain controller.

**Telnet path:**/Setup/NetBIOS/Support-Browsing

**Possible values:**

- Yes
- No

**Default**: Yes

## 2.17 DNS

This menu contains the domain-name system (DNS) configuration.

**SNMP ID:** 2.17

**Telnet path:** /Setup

### 2.17.1 Operating

Activates or deactivates DNS.

**SNMP ID:** 2.17.1

**Telnet path:** /Setup/DNS/Operating

**Possible values:**

- Yes
- No

**Default**: Yes

## 2.17.2 Domain

Device's own domain.

**SNMP ID:** 2.17.2

**Telnet path:** /Setup/DNS

**Possible values:**

- Max. 64 characters

**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.

**SNMP ID:** 2.17.3

**Telnet path:** /Setup/DNS

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.17.4 NetBIOS-Usage

The DNS server can resolve the names of the clients that are known to the NetBIOS router.

Use this switch to activate this option.

**SNMP ID:** 2.17.4

**Telnet path:** /Setup/DNS

**Possible values:**

- Yes

- No

**Default:** Yes

### 2.17.5 DNS-List

Enter the station names and the associated IP addresses here.

**SNMP ID:** 2.17.5

**Telnet path:** /Setup/DNS

## 2.17.5.1 Hostname

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.

**SNMP ID:** 2.17.5.1

**Telnet path:** /Setup/DNS/DNS-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.17.5.2 IP-Address

Enter the 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.

**SNMP ID:** 2.17.5.2

**Telnet path:** /Setup/DNS/DNS-List

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.17.5.3 IPV6-Address

Enter the 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.

**SNMP ID:** 2.17.5.3

**Telnet path:** /Setup/DNS/DNS-List

**Possible values:**

- Valid IPv6 address.

**Default:** Blank

### 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.

**Telnet path:**

**Setup** > **DNS** > **DNS-List**

**Possible values:**

0 to 65535

**Default:**

0

## 2.17.6 Filter-List

Use the DNS filter to block access to certain stations or domains.

**SNMP ID:** 2.17.6

**Telnet path:** /Setup/DNS

### 2.17.6.1 Idx.

Index for the filter entries.

**SNMP ID:** 2.17.6.1

**Telnet path:** /Setup/DNS/Filter-List

**Possible values:**

- Max. 4 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.17.6.2

**Telnet path:** /Setup/DNS/Filter-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.17.6.3 IP-Address

If you want this access restriction to only apply to a specific workstation or subnetwork, enter the IP address of the workstation or subnetwork here.

**SNMP ID:** 2.17.6.3

**Telnet path:** /Setup/DNS/Filter-List

**Possible values:**

- Valid IP address

**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.

**SNMP ID:** 2.17.6.4

**Telnet path:** /Setup/DNS/Filter-List

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

### 2.17.6.5 IPv6-Prefix

Using this setting you set the IPv6 addresses for which the device filters the domain. If you want to apply the filter to all IPv6 addresses, select the prefix `::/0`.

**Telnet path:**

**Setup** > **DNS** > **Filter-List**

**Possible values:**

Valid IPv6 prefix

**Default:**

### 2.17.6.6 Rtg-Tag

The routing tag determines which filters apply in each tag context.

**Telnet path:**

**Setup** > **DNS** > **Filter-List**

**Possible values:**

0 to 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.

**SNMP ID:** 2.17.7

**Telnet path:** /Setup/DNS

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.17.8

**Telnet path:** /Setup/DNS

#### 2.17.8.1 Hostname

Name of the station that registered via a register request.

**SNMP ID:** 2.17.8.1

**Telnet path:** /Setup/DNS/Dyn.-DNS-List

#### 2.17.8.2 IP-Address

IP address of the station that registered via a register request.

**SNMP ID:** 2.17.8.2

**Telnet path:** /Setup/DNS/Dyn.-DNS-List

**Possible values:**

- Valid IP address

## 2.17.8.3 Timeout

Lease period for this entry.

**SNMP ID:** 2.17.8.3

**Telnet path:** /Setup/DNS/Dyn.-DNS-List

## 2.17.8.4 IPV6-Address

Displays the IPv6 address of the corresponding host (if available).

**Telnet path:**
**Setup** > **DNS** > **Dyn.-DNS-List**

## 2.17.8.5 Network-name

Displays the name of the network in which the host is located.

**Telnet path:**
**Setup** > **DNS** > **Dyn.-DNS-List**

### 2.17.9 DNS-Destinations

Requests for certain domains can be explicitly forwarded to particular remote sites.

**SNMP ID:** 2.17.9

**Telnet 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.

**SNMP ID:** 2.17.9.1

**Telnet path:** /Setup/DNS/DNS-Destinations

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.17.9.2 Peer

Specify the remote station for DNS forwarding.

**SNMP ID:** 2.17.9.2

**Telnet path:** /Setup/DNS/DNS-Destinations

**Possible values:**

- Max. 31 characters

**Default:** Blank

### 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".

**Telnet path:**

**Setup** > **DNS** > **DNS-Destinations**

**Possible values:**

0 to 65535

**Default:**

0

### 2.17.10 Service-Location-List

Here you configure if and to which station certain services are to be resolved.

**SNMP ID:** 2.17.10

**Telnet 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 ID, station name, port)

- _sips._tcp.myhome.intern . 0
- _sip._tcp.myhome.intern myhost.myhome.intern 5060
- _sip._udp.myhome.intern [self] 5060

**Telnet path:** /Setup/DNS/Service-Location-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.17.10.2 Hostname

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).

**Telnet path:** /Setup/DNS/Service-Location-List

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.17.10.3 Port

The service port denotes the port number used for the defined service at the named client.

**Telnet path:** /Setup/DNS/Service-Location-List

**Possible values:**

- Max. 10 characters

**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.

**Telnet path:**

**Setup** > **DNS** > **Service-Location-List**

**Possible values:**

0 to 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.

**SNMP ID:** 2.17.11

**Telnet path:** /Setup/DNS

### 2.17.11.1 Service-Name

Name of the service.

**SNMP ID:** 2.17.11.1

**Telnet path:** /Setup/DNS/Dynamic-SRV-List

### 2.17.11.2 Hostname

Name of the station providing this service.

**SNMP ID:** 2.17.11.2

**Telnet path:** /Setup/DNS/Dynamic-SRV-List

### 2.17.11.3 Port

Port used to register this service.

**SNMP ID:** 2.17.11.3

**Telnet 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.

**SNMP ID:** 2.17.12

**Telnet path:** /Setup/DNS

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.17.13 Sub-Domains

Here a separate domain can be configured for each logical network.

**SNMP ID:** 2.17.13

**Telnet path:** /Setup/DNS

### 2.17.13.1 Network name

IP network for which a dedicated domain is to be defined.

**SNMP ID:** 2.17.13.1

**Telnet path:** /Setup/DNS/Sub-Domains

**Possible values:**

- Select from the list of defined IP networks.

**Default:** Blank

### 2.17.13.2 Sub-Domain

Sub-domain that is to be used for the selected IP network.

**SNMP ID:** 2.17.13.2

**Telnet path:** /Setup/DNS/Sub-Domains

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 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 and from the NetBIOS proxy, if necessary and if you allow it.

**Telnet path:**

**Setup** > **DNS**

**Possible values:**

Yes

No

**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.

**Telnet 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.

**Telnet path:**

**Setup** > **DNS** > **Tag-Configuration**

**Possible values:**

Valid routing tag, 1 to 65534

**Default:**

## 2.17.15.2 Active

Enables the DNS server of the device for the corresponding tag context.

**Telnet 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 and from the NetBIOS proxy, if necessary and if you allow it.

**Telnet path:**

**Setup** > **DNS** > **Tag-Configuration**

**Possible values:**

No

Yes

**Default:**

Yes

## 2.17.15.4 DHCP-usage

For the corresponding tag context, enables or disables the resolution of station names which have requested an IP address via DHCP.

**Telnet path:**

**Setup** > **DNS** > **Tag-Configuration**

**Possible values:**

No

Yes

**Default:**

Yes

## 2.17.15.5 NetBIOS usage

For the corresponding tag context, enables or disables the resolution of station names which are recognized by the NetBIOS router.

**Telnet path:**

**Setup** > **DNS** > **Tag-Configuration**

**Possible values:**

No

Yes

**Default:**

Yes

## 2.17.15.6 Resolve-Domain

For the corresponding tag context, enables or disables the response of DNS requests to its own domain with the IP address of the router.

**Telnet path:**

**Setup** > **DNS** > **Tag-Configuration**

**Possible values:**

No

Yes

**Default:**

Yes

# 2.18 Accounting

This menu contains the configuration of the Accounting.

**SNMP ID:** 2.18

**Telnet path:** /Setup

## 2.18.1 Operating

Turn accounting on or off.

**SNMP ID:** 2.18.1

**Telnet path:** /Setup/Accounting

**Possible values:**

- Yes
- 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.

**SNMP ID:** 2.18.2

**Telnet path:** /Setup/Accounting

**Possible values:**

- Yes
- No

## 2.18.3 Sort-by

Select here whether the data should be sorted in the accounting table according to connection times or data volume.

**SNMP ID:** 2.18.3

**Telnet path:** /Setup/Accounting

**Possible values:**

- Time
- Data

## 2.18.4 Current user

Displays an accounting list for all current users.

**SNMP ID:** 2.18.4

**Telnet path:** /Setup/Accounting

## 2.18.4.1 Username

Displays the username.

**SNMP ID:** 2.18.4.1

**Telnet path:** /Setup/Accounting/Current-User

## 2.18.4.3 Peer

Displays the name of the remote station.

**SNMP ID:** 2.18.4.3

**Telnet path:** /Setup/Accounting/Current-User

## 2.18.4.4 Conn.-Type

Displays the connection type (e.g. DSL connection)

**SNMP ID:** 2.18.4.4

**Telnet path:** /Setup/Accounting/Current-User

## 2.18.4.5 Rx-KBytes

The number of bytes received.

**SNMP ID:** 2.18.4.5

**Telnet path:** /Setup/Accounting/Current-User

### 2.18.4.6 Tx-KBytes

The number of bytes sent.

**SNMP ID:** 2.18.4.6

**Telnet path:** /Setup/Accounting/Current-User

### 2.18.4.8 Total-Time

Shows the total time of the corresponding connection.

**SNMP ID:** 2.18.4.8

**Telnet path:** /Setup/Accounting/Current-User

### 2.18.4.9 Connections

Displays the number of connections.

**SNMP ID:** 2.18.4.9

**Telnet path:** /Setup/Accounting/Current-User

## 2.18.5 Accounting-List

Information on connections between clients in the local network and various remote sites is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

**SNMP ID:** 2.18.5

**Telnet path:** /Setup/Accounting

### 2.18.5.1 Username

Displays the username.

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.3 Peer

Displays the name of the remote station.

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.4 Conn.-Type

Displays the connection type (e.g. DSL connection)

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.5 Rx-KBytes

The number of bytes received.

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.6 Tx-KBytes

The number of bytes sent.

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.8 Total-Time

Shows the total time of the corresponding connection.

**Telnet path:**/Setup/Accounting/Accounting-List

### 2.18.5.9 Connections

Displays the number of connections.

**Telnet path:**/Setup/Accounting/Accounting-List

## 2.18.6 Delete-Accounting-List

This option allows you to delete the parameters.

**SNMP ID:** 2.18.6

**Telnet path:** /Setup/Accounting

### 2.18.8 Time-Snapshot

When configuring the snapshot, the interval is set at which the accounting data are temporarily saved into a snapshot.

**SNMP ID:** 2.18.8

**Telnet path:** /Setup/Accounting

#### 2.18.8.1 Index

Displays the system's internal index.

**Telnet path:**/Setup/Accounting/Time-Snapshot

**Default:** 1

#### 2.18.8.2 Operating

Turn intermediate storage of accounting data on or off.

**Telnet 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.

**Telnet 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'.

**Telnet path:**/Setup/Accounting/Time-Snapshot

**Possible values:**

- 0 to 31

**Default:** 1

### 2.18.8.5 DayOfWeek

The weekday on which caching is performed. Only relevant if the interval is 'weekly'.

**Telnet path:**/Setup/Accounting/Time-Snapshot

**Possible values:**

- 0 to 7

**Default:** Unknown

### 2.18.8.6 Hour

The hour of day at which caching will be performed.

**Telnet path:**/Setup/Accounting/Time-Snapshot

**Possible values:**

- 0 to 23

**Default:** 0

### 2.18.8.7 Minute

The minute in which caching will take place

**Telnet path:**/Setup/Accounting/Time-Snapshot

**Possible values:**

- 0 to 59

**Default:** 0

## 2.18.9 Last snapshot

Displays the last snapshot.

**SNMP ID:** 2.18.9

**Telnet path:** /Setup/Accounting

### 2.18.9.1 Username

Displays the username.

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.3 Peer

Displays the name of the remote station.

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.4 Conn.-Type

Displays the connection type (e.g. DSL connection)

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.5 Rx-KBytes

The number of bytes received.

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.6 Tx-KBytes

The number of bytes sent.

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.8 Total-Time

Shows the total time of the corresponding connection.

**Telnet path:**/Setup/Accounting/Last-Snapshot

### 2.18.9.9 Connections

Displays the number of connections.

**Telnet path:**/Setup/Accounting/Last-Snapshot

## 2.18.10 Discriminator

This is where you can select the feature according to which accounting data are to be gathered. MAC address: The data are collected according to the client's MAC address. IP address: The data are collected according to the client's IP address. --> see information

**SNMP ID:** 2.18.10

**Telnet path:** /Setup/Accounting

**Possible values:**

- MAC address
- IP address

**Note:** When varying IP addresses are in use, e.g. when using a DHCP server, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users. Conversely, with this setting, data can be separated for clients that are behind another

router and therefore appear in the accounting list with the same MAC address as the router.

# 2.19 VPN

This menu contains the configuration of the Virtual Private Network (VPN).

**Telnet path:**

**Setup**

## 2.19.3 Isakmp

This menu contains the configuration of the Isakmp.

**Telnet 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.

**SNMP ID:** 2.19.3.4

**Telnet 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 default value is '5'. 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.

**SNMP ID:** 2.19.3.4.1

**Telnet path:** /Setup/VPN/Isakmp/Timer

**Possible values:**

- Maximum 5 characters

**Default:** 5

### 2.19.3.4.2 Retr-Tim

**Note:** 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.

**SNMP ID:** 2.19.3.4.2

**Telnet path:** /Setup/VPN/Isakmp/Timer

### 2.19.3.4.3 Retr-Tim-Usec

**Note:** 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.

**SNMP ID:** 2.19.3.4.3

**Telnet path:** /Setup/VPN/Isakmp/Timer

### 2.19.3.4.4 Retr-Tim-Max

**Note:** 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.

**SNMP ID:** 2.19.3.4.4

**Telnet path:** /Setup/VPN/Isakmp/Timer

#### 2.19.3.4.5 Exp-Tim

Maximum duration of the IKE negotiation phase in seconds.

**SNMP ID:** 2.19.3.4.5

**Telnet path:** /Setup/VPN/Isakmp/Timer

**Possible values:**

- 0 to 65535

**Default:** 30 seconds

**Note:** 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.

#### 2.19.3.4.6 Idx.

The table contains only one line, so the index only has the value '1'.

**SNMP ID:** 2.19.3.4.6

**Telnet path:** /Setup/VPN/Isakmp/Timer

### 2.19.3.29 DH-Groups

This menu contains the configuration for the precalculation of DH keys.

**Telnet path:**

**Setup** > **VPN** > **Isakmp**

#### 2.19.3.29.1Precalculation

This option enables or disables the precalculation of DH keys.

**Telnet 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.

**Telnet path:**

**Setup** > **VPN** > **Isakmp** > **DH-Groups**

#### *2.19.3.29.2.1 DH-Group*

This value displays the corresponding DH group.

**Telnet path:**

**Setup** > **VPN** > **Isakmp** > **DH-Groups** > **Group-config**

**Possible values:**

**Selection from the list of predefined DH groups**

#### *2.19.3.29.2.2 Precalculation target*

This value specifies the number of DH keys to be calculated for this DH group.

**Note:** 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.

**Telnet path:**

**Setup** > **VPN** > **Isakmp** > **DH-Groups** > **Group-config**

**Possible values:**

0 to 999999999

**Default:**

0

## 2.19.4 Proposals

This menu contains the configuration of the Proposals.

**SNMP ID:** 2.19.4

**Telnet path:** /Setup/VPN

## 2.19.4.9 IKE-Proposal-Lists

Here you can display and add IKE proposal lists.

**SNMP ID:** 2.19.4.9

**Telnet path:** /Setup/VPN/Proposals

### 2.19.4.9.1 IKE-Proposal-Lists

Name for the combination of IKE proposals

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.19.4.9.2 IKE-Proposal-1

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

### 2.19.4.9.3 IKE-Proposal-2

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.4 IKE-Proposal-3

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.5 IKE-Proposal-4

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.6 IKE-Proposal-5

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.7 IKE-Proposal-6

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.8 IKE-Proposal-7

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

#### 2.19.4.9.9 IKE-Proposal-8

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IKE-Proposal-Lists

**Possible values:**

- Select from the defined IKE proposals

**Default:** Blank

### 2.19.4.10 IPSEC-Proposal-Lists

Here you combine previously-defined proposals to form proposal lists.

**SNMP ID:** 2.19.4.10

**Telnet path:** /Setup/VPN/Proposals

#### 2.19.4.10.1 IPSEC-Proposal-Lists

Name for the combination of IPSec proposals

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.19.4.10.2 IPSEC-Proposal-1

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.3 IPSEC-Proposal-2

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.4 IPSEC-Proposal-3

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.5 IPSEC-Proposal-4

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.6 IPSEC-Proposal-5

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.7 IPSEC-Proposal-6

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.8 IPSEC-Proposal-7

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

### 2.19.4.10.9 IPSEC-Proposal-8

Proposal to be used for this list.

**Telnet path:**/Setup/VPN/Proposals/IPSEC-Proposal-Lists

**Possible values:**

- Select from the defined IPSec proposals

**Default:** Blank

## 2.19.4.11 IKE

In this table you can define the proposals for administration of the SA negotiation.

**SNMP ID:** 2.19.4.11

**Telnet path:** /Setup/VPN/Proposals

### 2.19.4.11.1 Name

Name for the combinations of IKE parameters that should be used as the proposal.

**SNMP ID:** 2.19.4.11.1

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- Max. 64 characters

**Default:** Blank

**Note:** The Internet Key Exchange (IKE) is a protocol for authentication and key exchange.

### 2.19.4.11.2 IKE-Crypt-Alg

Encryption algorithm for this proposal

**SNMP ID:** 2.19.4.11.2

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- AES
- Blowfish
- CAST128

- 3DES
- DES
- NULL

**Default:** AES-CBC

### 2.19.4.11.3 IKE-Crypt-Keylen

Key length for this proposal

**SNMP ID:** 2.19.4.11.3

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- 0 to 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.

**Telnet 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

**SNMP ID:** 2.19.4.11.5

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- Pre-shared 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

**SNMP ID:** 2.19.4.11.6

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- 0 to 65535

**Default:** 8000 seconds

**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.

**SNMP ID:** 2.19.4.11.7

**Telnet path:** /Setup/VPN/Proposals/IKE

**Possible values:**

- 0 to 65535

**Default:** 0 kBytes

**Special values:** 0: No limit on data volume

## 2.19.4.12 IPSEC

You define the defaults for encryption, authentication or compression here.

**SNMP ID:** 2.19.4.12

**Telnet path:** /Setup/VPN/Proposals

### 2.19.4.12.1 Name

Name for the combinations of IPSec parameters that should be used as the proposal.

**SNMP ID:** 2.19.4.12.1

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- Max. 64 characters

**Default:** Blank

**Note:** 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.

### 2.19.4.12.2 Encaps-Mode

Connection mode selection

**SNMP ID:** 2.19.4.12.2

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- Transport: In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted. The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for example for the remote configuration of a router. It cannot be used for the connectivity of networks via the Internet – this would require a new IP header with the

public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

- Tunnel: In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

**Default:** Tunnel

### 2.19.4.12.3 ESP-Crypt-Alg

Encryption algorithm for this proposal

**SNMP ID:** 2.19.4.12.3

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NULL

**Default:** AES-CBC

### 2.19.4.12.4 ESP-Crypt-Keylen

Key length for this proposal

**SNMP ID:** 2.19.4.12.4

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- 0 to 65535

**Default:** 128

### 2.19.4.12.5 ESP-Auth-Alg

ESP authentication method for this proposal

**Telnet path:**

**Setup** > **VPN** > **Proposals** > **IPSEC**

**Possible values:**

No authentication

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

**Default:**

No authentication

### 2.19.4.12.6 AH-Auth-Alg

AH authentication method for this proposal

**Telnet path:**

**Setup** > **VPN** > **Proposals** > **IPSEC**

**Possible values:**

No authentication

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

**Default:**

No authentication

### 2.19.4.12.7 IPCOMP-Alg

Compression method for this proposal

**SNMP ID:** 2.19.4.12.7

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- No IPCOMP
- Deflate
- LZS

**Default:** No IPCOMP

#### 2.19.4.12.8 Lifetime-Sec

Validity of the connections negotiated with this proposal with respect to connection duration

**SNMP ID:** 2.19.4.12.8

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- 0 to 65535

**Default:** 8000 seconds

**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.

**SNMP ID:** 2.19.4.12.9

**Telnet path:** /Setup/VPN/Proposals/IPSEC

**Possible values:**

- 0 to 65535

**Default:** 0 kBytes

**Special values:** 0: No limit on data volume

### 2.19.5 Certificates-and-Keys

This menu contains the configuration of the certificates and keys.

**SNMP ID:** 2.19.5

**Telnet 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.

**Telnet path:** /Setup/VPN/Certificates-and-Keys

### 2.19.5.3.1 Name

Name for the combination of identities and keys

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.19.5.3.2 Remote-Identity

Remote ID that the entered key is to be valid for.

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.19.5.3.3 Shared-Sec

Key/secret that should apply to this combination.

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.19.5.3.4 Shared-Sec-File

[obsolete, not used: File with PSK]

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

### 2.19.5.3.5 Remote-ID-Type

Type of remote ID that the entered key is to be valid for.

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- No identity
- IP address
- Domain name (FQDN)
- E-mail address (FQUN)
- ASN.1-Distinguished Name

**Default:** No identity

### 2.19.5.3.6 Local-ID-Type

Type of local ID that the entered key is to be valid for.

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- No identity
- IP address
- Domain name (FQDN)
- E-mail address (FQUN)
- ASN.1-Distinguished Name

**Default:** No identity

### 2.19.5.3.7 Local-Identity

Local ID that the entered key is to be valid for.

**Telnet path:** /Setup/VPN/Certificates-and-Keys/IKE-Keys

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.19.7 Layer

Here you define further parameters for individual VPN connections.

**Telnet path:**

**Setup** > **VPN**

## 2.19.7.1 Name

Name for the combination of connection parameters

**SNMP ID:** 2.19.7.1

**Telnet path:** /Setup/VPN/Layer

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 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.

**Telnet 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.

**Telnet 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

IKE proposal list for this connection.

**SNMP ID:** 2.19.7.5

**Telnet path:** /Setup/VPN/Layer

**Possible values:**

- Select from the list of defined IKE proposal lists.

**Default:** Blank

### 2.19.7.6 IPSEC-Prop-List

IKE key for this connection.

**SNMP ID:** 2.19.7.6

**Telnet path:** /Setup/VPN/Layer

**Possible values:**

- Select from the list of defined IKE keys.

**Default:** Blank

### 2.19.7.7 IKE-Key

IPsec proposal list for this connection.

**SNMP ID:** 2.19.7.7

**Telnet path:** /Setup/VPN/Layer

**Possible values:**

- Select from the list of defined IPSec proposal lists.

**Default:** Blank

## 2.19.8 Operating

Switches the VPN module on or off.

**SNMP ID:** 2.19.8

**Telnet path:** /Setup/VPN

**Possible values:**

- Activated
- Deactivated

**Default:** Deactivated

### 2.19.9 VPN-Peers

In this table you define the VPN connections to be established by your device.

**SNMP ID:** 2.19.9

**Telnet path:** /Setup/VPN

## 2.19.9.1 Peer

Name of the VPN connection.

**SNMP ID:** 2.19.9.1

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

## 2.19.9.2 Extranet address

In HiLCOS 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 HiLCOS version 9.10, masquerading uses the entry under **Setup** > **WAN** > **IP-List** in the field **Masq.-IP-Addr.**.

**Telnet path:**

**Setup** > **VPN** > **VPN-Peers**

**Possible values:**

Max. 15 characters from `[0-9].`

**Default:**
*empty*

## 2.19.9.4 Layer

Combination of connection parameters (PFS, IKE and IPSec parameters) that should be used for this connection.

**SNMP ID:** 2.19.9.4

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Select from the list of defined connection parameters.

**Default:** Blank

## 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.

**SNMP ID:** 2.19.9.5

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- No dynamic VPN
- Dynamic VPN: A connection is established to transmit IP addresses
- Dynamic VPN: IP addresses are transmitted without establishing a connection if possible:
- Dynamic VPN: An ICMP packet is sent to the remote site to transmit the IP address
- Dynamic VPN: A UDP packet is sent to the remote site to transmit the IP address

**Default:** No dynamic VPN

## 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.

**SNMP ID:** 2.19.9.6

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- 0 to 9999

**Default:** 0

**Special values:** With the value 9999, connections are established immediately and without a time limit.

## 2.19.9.7 IKE-Exchange

Selects the IKE exchange mode

**SNMP ID:** 2.19.9.7

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Main mode
- Aggressive mode

**Default:** Main mode

**Note:** 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.

## 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.

**SNMP ID:** 2.19.9.8

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.19.9.9 Rule creation

On/off switch and type of rule creation

**SNMP ID:** 2.19.9.9

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Off: No VPN rule is created for the remote site.
- Automatic: Automatically created VPN rules connect the local IP networks with the IP networks entered into the routing table for the remote site.
- Manually: VPN rules are only created for the remote site for IP network relationships specified "Manually" in the firewall configuration.

**Default:** Automatic

## 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.

**SNMP ID:** 2.19.9.10

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- 0 to 9999 numerical characters

**Default:** 0

**Note:** 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.

## 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.

**SNMP ID:** 2.19.9.11

**Telnet 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

**Note:** 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.

## 2.19.9.12 XAUTH

Enables the use of XAUTH for the VPN remote site selected.

**SNMP ID:** 2.19.9.12

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- 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.
- Off: No XAUTH authentication is performed for the connection to this remote site.

**Default:** Off

**Note:** If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

## 2.19.9.13 SSL-Encaps.

With this option you activate IPsec-over-HTTPS technology when actively establishing a connection to this remote site.

**SNMP ID:** 2.19.9.13

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- Yes, No

**Default:** No

**Note:** 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.

## 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.

**SNMP ID:** 2.19.9.15

**Telnet path:** /Setup/VPN/VPN-Peers

**Possible values:**

- 0 to 65535

**Default:** 0

## 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.

**SNMP ID:** 2.19.10

**Telnet path:** /Setup/VPN

**Possible values:**

- Select from the list of defined IKE proposal lists.

**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.

**Telnet 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.

**SNMP ID:** 2.19.12

**Telnet path:** /Setup/VPN

## 2.19.12.1 Peer

Name of the VPN connection that works with the additional gateway defined here.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Select from the list of defined VPN connections.

**Default:** Blank

## 2.19.12.2 Gateway-1

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.3 Gateway-2

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

### 2.19.12.4 Gateway-3

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

### 2.19.12.5 Gateway-4

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

### 2.19.12.6 Gateway-5

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

### 2.19.12.7 Gateway-6

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.8 Gateway-7

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.9 Gateway-8

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.10 Begin-With

Here you select the first gateway that is to be used for establishing the VPN connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- First: Start with the first entry in the list.
- Random: Selects a random entry from the list.

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

**Default:** Last used

## 2.19.12.11 Rtg-Tag-1

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.12 Rtg-Tag-2

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.13 Rtg-Tag-3

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.14 Rtg-Tag-4

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.15 Rtg-Tag-5

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.16 Rtg-Tag-6

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.17 Rtg-Tag-7

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.18 Rtg-Tag-8

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 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.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 64 characters

**Default:** Blank

## 2.19.12.20 Gateway-10

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.21 Gateway-11

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.22 Gateway-12

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.23 Gateway-13

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.24 Gateway-14

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.25 Gateway-15

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.26 Gateway-16

DNS name or IP address of the remote gateway to be used as an alternative to the connection.

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.27 Rtg-Tag-9

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.28 Rtg-Tag-10

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.29 Rtg-Tag-11

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.30 Rtg-Tag-12

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.31 Rtg-Tag-13

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.32 Rtg-Tag-14

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.33 Rtg-Tag-15

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 65535

**Default:** 0

## 2.19.12.34 Rtg-Tag-16

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

**Telnet path:** /Setup/VPN/Additional-Gateways

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-17

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.36 Rtg-Tag-17

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-17

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-18

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.38 Rtg-Tag-18

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-18

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-19

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.40 Rtg-Tag-19

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-19

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-20

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.42 Rtg-Tag-20

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-20

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-21

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.44 Rtg-Tag-21

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-21

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-22

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.46 Rtg-Tag-22

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-22

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-23

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.48 Rtg-Tag-23

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-23

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-24

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.50 Rtg-Tag-24

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-24

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-25

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.52 Rtg-Tag-25

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-25

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-26

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.54 Rtg-Tag-26

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-26

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-27

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.56 Rtg-Tag-27

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-27

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-28

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.58 Rtg-Tag-28

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-28

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-29

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.60 Rtg-Tag-29

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-29

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-30

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.62 Rtg-Tag-30

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-30

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-31

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.64 Rtg-Tag-31

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-31

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Gateway-32

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 2.19.12.66 Rtg-Tag-32

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

**Telnet path:**/Setup/VPN/Certificates-and-Keys/Additional-Gateways/Rtg-Tag-32

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.19.13

**Telnet path:** /Setup/VPN

**Possible values:**

- Select from the list of defined IKE proposal lists.

**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.

**Telnet 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.

**SNMP ID:** 2.19.16

**Telnet path:** /Setup/VPN

**Possible values:**

- On
- Off

**Default:** Off

**Note:** 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.

**Note:** 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.

## 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).

**SNMP ID:** 2.19.17

**Telnet path:** /Setup/VPN

**Possible values:**

- On
- Off

**Default:** Off

## 2.19.19 QuickMode-Proposal-List-Default

This IPSec proposal list is used for simplified dial-in with certificates.

**SNMP ID:** 2.19.19

**Telnet path:** /Setup/VPN

**Possible values:**

- Select from the list of defined IPSec proposal lists.

**Default:** ESP_TN

## 2.19.20 QuickMode-PFS-Group-Default

This IPSec group is used for simplified dial-in with certificates.

**Telnet 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.

**SNMP ID:** 2.19.21

**Telnet path:** /Setup/VPN

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.19.22

**Telnet path:** /Setup/VPN

**Possible values:**

- On
- Off

**Default:** Off

**Note:** 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.

## 2.19.23 Establish-SAs-Collectively

Security Associations (SAs) are the basis for establishing a VPN tunnel between two networks. The establishment of Security Associations is normally initiated by an IP packet which is to be sent from a source network to a destination network.

The establishment of Security Associations is normally initiated by an IP packet which is to be sent from a source network to a destination network. This allows the setup of network relationships to be precise controlled according to the application.

**SNMP ID:** 2.19.23

**Telnet path:** /Setup/VPN

**Possible values:**

- Separately: Only the SA which corresponds explicitly to a packet waiting for transfer is to be established.
- Collectively: All SAs defined in the device will be established.

- Collectively with KeepAlive All of the defined SAs will be established for remote sites in the VPN connection list with a hold time set to '9999' (Keep Alive).

**Default:** Separately

## 2.19.24 Max-Concurrent-Connections

This setting determines how many VPN connections the device can establish.

**Telnet path:** /Setup/VPN/Max-Concurrent-Connections

**Possible values:**

- The maximum value is limited by the relevant license.

**Default:** 0

**Note:** 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 Flexibler-ID-Comparison

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

**SNMP ID:** 2.19.25

**Telnet path:** /Setup/VPN

**Possible values:**

- Yes
- No

**Default:** No

**Note:** Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

## 2.19.26 NAT-T-Port-for-Rekeying

This item sets whether the IKE packets are sent to port 500 (no) or the port 4500 (yes) during rekeying.

**Telnet path:** /Setup/VPN/NAT-T-Port-For-Rekeying

**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).

**SNMP ID:** 2.19.27

**Telnet path:** /Setup/VPN

**Possible values:**

- Yes, No

**Default:** No

**Note:** 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.

## 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.

**Telnet path:**

**Telnet path:Setup** > **Vpn** > **myVPN**

**Possible values:**

Max. 5 numbers

**Default:**

0

**Special values:**

A value of 0 disables replay detection.

# 2.20 LAN-Bridge

This menu contains the settings for the LAN bridge.

**SNMP ID:** 2.20

**Telnet path:** /Setup

## 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Version

**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.

**Telnet path:** /Setup/LAN-Bridge/Bridge-Priority

**Possible values:**

- Max. 5 numerical characters

**Default:** 32768

**Note:** 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.

## 2.20.4 Encapsulation-Table

This table is used to add the encapsulation methods.

**SNMP ID:** 2.20.4

**Telnet 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.

**Telnet 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.

**Telnet 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 'outdated'. 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).

**SNMP ID:** 2.20.5

**Telnet path:** /Setup/LAN-Bridge/Max-Age

**Possible values:**

- Max. 5 numerical characters

**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.

**SNMP ID:** 2.20.6

**Telnet path:** /Setup/LAN-Bridge/Hello-Time

**Possible values**:

- Max. 5 numerical characters

**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.

**SNMP ID:** 2.20.7

**Telnet path:** /Setup/LAN-Bridge/Forward-Delay

**Possible values:**

- Max. 5 numerical characters

**Default:** 6

## 2.20.8 Isolierter-Mode

This item allows connections to be switched on or off, such as those between layer-2 forwarding and the LAN interfaces.

**SNMP ID:** 2.20.8

**Telnet path:** /Setup/LAN-Bridge

**Possible values:**

- Bridge or router (isolated mode)

**Default:** Bridge

**Note:** 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.

## 2.20.10 Protocol-Table

You can add the protocols to be used over the LAN bridge here.

**SNMP ID:** 2.20.10

**Telnet 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Max. 15 characters

**Default:** Blank

## 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- 4-digit hexadecimal number

**Default:** Blank

## 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 pro-

tocol 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".

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Maximum 65,535

**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 '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".

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Maximum 65,535

**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".

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Maximum 65,535

**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 following abbreviations: P2P-4~P2P-10. If no interface is specified here, the selected action will never be executed.

**Telnet 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

**Default:** Blank

## 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Transmit
- Drop
- Redirect

**Default:** Drop packets

## 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Valid IP address

**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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- 12-digit hexadecimal number

**Default:** Blank

## 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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Valid IP address

**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.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.20.10.12 DHCP-Src-MAC

meine Übersetzung: This setting decides whether matching of the rule shall depend on a packet’s source MAC address, i.e. whether it is the MAC address of a host that received its IP address via DHCP.

Aus anderer Quelle (Aurelia): DHCP tracking on a particular (W)LAN interface only takes place when protocol filters for the interface have been defined with the parameter "IP allocated by DHCP" set to Yes or No. Additionally, a network can be specified for a filter rule. However, if a rule has the parameter "IP allocated by DHCP" set to Yes, then a given network could be ignored.

**Telnet path:**/Setup/LAN-Bridge/Protocol-Table

**Possible values:**

- Irrelevant
- No
- Yes

**Default:** Irrelevant

## 2.20.11 Port-Data

This table can be used to set further bridge parameters for each port.

**SNMP ID:** 2.20.11

**Telnet path:** /Setup/LAN-Bridge

## 2.20.11.2 Port

Selects the port for which the spanning tree parameters are to be set.

**SNMP ID:** 2.20.11.2

**Telnet path:** /Setup/LAN-Bridge/Port-Data

**Possible values:**

- Select from the list of the device's logical interfaces, e.g. LAN-1, WLAN-1 or P2P-1-1

## 2.20.11.3 Active

This can be used to block a port completely, i.e. the port will always have the 'disabled' status.

**SNMP ID:** 2.20.11.3

**Telnet path:** /Setup/LAN-Bridge/Port-Data

**Possible values:**

- Up
- Down

**Default:** Activated

## 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.

**SNMP ID:** 2.20.11.5

**Telnet path:** /Setup/LAN-Bridge/Port-Data

**Possible values:**

- BRG-1 to BRG-8
- None

**Default:** BRG - 1

**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.

**Note:** 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.

## 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.

**SNMP ID:** 2.20.11.6

**Telnet path:** /Setup/LAN-Bridge/Port-Data

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.20.11.7

**Telnet path:** /Setup/LAN-Bridge/Port-Data

**Possible values:**

- Automatic
- Yes
- Off

**Default:** Automatic

## 2.20.11.9 Private mode

You have the option to enable or disable the private mode for each individual interface.

**Telnet 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 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.

**SNMP ID:** 2.20.12

**Telnet path:** /Setup/LAN-Bridge

**Possible values:**

- 1 to 99,999 minutes

**Default:** Max. validity 6,000 min., default validity: 500 min.

## 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).

**Telnet path:**/Setup/LAN-Bridge/Priority-Mapping

## 2.20.13.1 Name

Enter a name for a combination of DSCP value and priority.

**Telnet path:**/Setup/LAN-Bridge/Priority-Mapping/Name

**Possible values:**

- Maximum 16 alphanumerical characters

**Default:** Blank

## 2.20.13.2 DSCP-Value

Enter the DSCP value that is used for this priority assignment.

**Telnet path:**/Setup/LAN-Bridge/Priority-Mapping/DSCP-Value

**Possible values:**

- Numerical characters from 0 to 255

**Default:** 0

## 2.20.13.3 Priority

Enter the priority that is used for this priority assignment.

**Telnet path:**/Setup/LAN-Bridge/Priority-Mapping/Priority

**Possible values:**

- Best-Effort
- Background
- Two

- Excellent-Effort
- Controlled latency
- Video
- Voice
- Network-Control

**Default:** Best-Effort

### 2.20.20 Spannning-Tree

This menu contains the settings for the spanning tree.

**SNMP ID:** 2.20.20

**Telnet 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.

**SNMP ID:** 2.20.20.1

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Up
- Down

**Default:** Disabled

## 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.

**SNMP ID:** 2.20.20.2

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Maximum 65,535

**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.

**SNMP ID:** 2.20.20.5

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Max. 65535 seconds

**Default:** 20 seconds

## 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.

**SNMP ID:** 2.20.20.6

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Max. 32768 seconds

**Default:** 2 seconds

## 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. o not change this value without detailed knowledge of spanning tree, since it may increase the risk of temporary loops in the network.

**SNMP ID:** 2.20.20.7

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Max. 32768 seconds

**Default:** 6 seconds

## 2.20.20.11 Port-Data

This table can be used to set further spanning-tree parameters for each port.

**SNMP ID:** 2.20.20.11

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

### 2.20.20.11.2 Port

The name of the LAN interface.

**Telnet 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.

**Telnet path:**/Setup/LAN-Bridge/Spanning-Tree/Port-Data

**Possible values:**

- Maximum 255

**Default:** 128

**Note:** 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.

### 2.20.20.11.6 Edge-Port

A port can be labeled as an edge port

**Telnet path:**/Setup/LAN-Bridge/Spanning-Tree/Port-Data

**Possible values:**

- On
- Off

**Default:** No label

### 2.20.20.11.7 Path-Cost-Override

Specifies the influence of path cost.

**Telnet path:**/Setup/LAN-Bridge/Spanning-Tree/Port-Data

**Possible values:**

- Maximum 4,294,967,295

**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.

**SNMP ID:** 2.20.20.12

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Classic
- Rapid

**Default:** Classic

**Note:** 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.

## 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.)

**SNMP ID:** 2.20.20.13

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Maximum 999

**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.

**SNMP ID:** 2.20.20.14

**Telnet path:** /Setup/LAN-Bridge/Spanning-Tree

**Possible values:**

- Classic
- Rapid

**Default:** Classic

## 2.20.30 IGMP-Snooping

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

## 2.20.30.1 Enabled

Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

**Note:** 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 snooping function, i.e. it deltes all dynamically learned values (memberships, router-port properties).

### Telnet path:

**Setup** > **LAN-Bridge** > **IGMP-Snooping**

### Possible values:

No

Yes

Auto

### Default:

No

## 2.20.30.2 Port-Settings

This table defines the port-related settings for IGMP snooping.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

#### 2.20.30.2.1 Port

The port for which the settings apply.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping/Port-Settings/Port

**Possible values:**

- Selects a port from the list of those available in the device.

#### 2.20.30.2.2 Router-Port

This option defines the port's behavior.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping/Port-Settings/Router-Port

**Possible values:**

- Yes: This port will always work as a router port, irrespective of IGMP queries or router messages received at this port.
- No: This port will never work as a router port, irrespective of IGMP queries or router messages received at this port.
- Auto: This port will work as a router port if IGMP 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 the 224.0.0.x range and for which neither static memberships were defined nor were dynamic memberships learned.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** 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 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.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

**Name**

Name of the querier instance

Possible values:

- 8 alphanumerical characters.

Default: Blank

**Operating**

Activates or deactivates the querier instance

Possible values:

- Yes
- No

Default: No

**Bridge group**

Limits the querier instance to a certain bridge group.

Possible values:

- Select from the list of available bridge groups.

Default: None

Special values: If bridge group is set to "none", the IGMP queries will the sent via all bridge groups.

**VLAN-ID**

Limits the querier instance to a certain VLAN.

Possible values:

- 0 to 4096.

Default: 0

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

### 2.20.30.4.1 Name

Name of the querier instance

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Simulated-Queriers/Name

**Possible values:**

- 8 alphanumerical characters.

**Default:** Blank

### 2.20.30.4.2 Operating

Activates or deactivates the querier instance

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Simulated-Queriers/Operating

**Possible values:**

- Yes
- No

**Default:** No

### 2.20.30.4.3 Bridge-Group

Limits the querier instance to a certain bridge group.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Simulated-Queriers/Bridge-Group

**Possible values:**

- Select from the list of available bridge groups.
- None

**Special values:** If bridge group is set to "none", the IGMP queries will the sent via all bridge groups.

**Default:** None

#### 2.20.30.4.4 VLAN-Id

Limits the querier instance to a certain VLAN.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Simulated-Queriers/VLAN-Id

**Possible values**:

- 0 to 4096

**Special values:** If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

**Default:** 0

### 2.20.30.5 Query-Interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, 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 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)".

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

**Possible values:**

- 10-figure number greater than 0

**Default:** 125

**Note:** The query interval must be greater than the query response interval.

## 2.20.30.6 Query-Response-Interval

Interval in seconds influencing the timing between IGMP 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 queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

**Possible values:**

- 10-figure number greater than 0

**Default:** 10

**Note:** The query response interval must be less than the query interval.

## 2.20.30.7 Robustness

This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

**Possible values:**

- 10-figure number greater than 0

**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.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**Address**

The IP address of the manually defined multicast group.

Possible values:

- Valid IP multicast address

Default: Blank

**VLAN-ID**

The VLAN ID which is to support this static member. Each IP multicast address can have multiple entries with different VLAN IDs.

Possible values:

- 0 to 4096

Default: 0

Special values: If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

**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.

Possible values:

- Yes
- No

Default: Yes

**Static-Members**

These ports will always be the destination for packets with the corresponding IP multicast address, irrespective of any Join messages received.

Possible values:

- Comma-separated list of the desired ports, max. 215 alphanumerical characters

Default: Blank

#### 2.20.30.8.1 Address

The IP address of the manually defined multicast group.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Address

**Possible values:**

- Valid IP multicast address

**Default:** Blank

#### 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.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Static-Members

**Possible values:**

- Comma-separated list of the desired ports, max. 215 alphanumerical characters

**Default:** Blank

#### 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.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Static-Members/VLAN-Id

**Possible values:**

- 0 to 4096

**Special values:** If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

**Default:** 0

#### 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.

**Telnet path:**/Setup/LAN-Bridge/IGMP-Snooping/Static-Members/Allow-Learning

**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-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 queries.

**Telnet path:** /Setup/LAN-Bridge/IGMP-Snooping

**WEBconfig English:** Setup/LAN-Bridge/IGMP-Snooping

**Possible values:**

- 4 to 180 seconds

**Default:** 20

### 2.20.40 DHCP-Snooping

Here you can configure DHCP snooping for each interface.

**Telnet path:**

**Setup** > **LAN-Bridge**

## 2.20.40.1 Port

Indicates the physical or logical interface to which this DHCP-snooping configuration applies.

**Telnet 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**.

**Notice:** If these two fields are empty, the DHCP relay agent does not add any 'Relay Agent Info' to the data packets.

**Telnet 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.

**Telnet 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**.

**Telnet 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**.

**Telnet 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.

**Telnet path:**
**Setup** > **LAN-Bridge**

## 2.20.41.1 Port

Indicates the physical or logical interface to which this DHCPv6-snooping configuration applies.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Important:** 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.

**Note:** 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**.

**Telnet 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**.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet path:**

**Setup** > **LAN-Bridge**

## 2.20.42.1 Port

Indicates the physical or logical interface to which this RA-snooping configuration applies.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **LAN-Bridge**

## 2.20.43.1 Port

Indicates the physical or logical interface to which this PPPoE-snooping configuration applies.

**Telnet 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**.

**Note:** If these two fields are empty, the PPPoE intermediate agent does not add a PPPoE tag to the data packets.

**Telnet 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**.

**Telnet 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**.

**Telnet 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.

**Telnet 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

### 2.20.248 L2-Firewall

Make the settings for the L2 Firewall at this point.

**Telnet path:**

> **Setup** > **LAN-Bridge**

## 2.20.248.1 Config

Make the settings for the L2 Firewall configuration at this point.

**Telnet path:**

> **Setup** > **LAN-Bridge** > **L2-Firewall**

#### 2.20.248.1.1 Maximum-Number-Of-Rules

Specify the maximum number of L2 Firewall rules here.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config**

**Possible values:**
10 characters `[0-9]`

**Default:**
1000

### 2.20.248.1.10 Bridge-Mapping

Here is the table for bridge mapping.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config**

#### *2.20.248.1.10.1 Bridge-Index*

Select the bridge group here.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Bridge Mapping**

**Possible values:**
**Selection from available bridge groups**

#### *2.20.248.1.10.2 Enable*

Enable or disable the bridge group here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Bridge-Mapping**

**Possible values:**

**No**
Bridge group off

**Yes**
Bridge group on

**Default:**
No

### *2.20.248.1.10.3 Filter-Management*

Here you activate the L2 Firewall filter for frames addressed to the management address of the device.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Bridge-Mapping**

**Possible values:**

**No**
Filter for management frames off

**Yes**
Filter for management frames on

**Default:**
No

## 2.20.248.1.11 Rule-Table

Here is the rule table.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config**

### *2.20.248.1.11.1 Rule-Index*

Specify the rule index here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

Max. 4 characters `[0-9]`

**Default:**

*empty*

### *2.20.248.1.11.2 Source-Address*

Specify the source address here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

IPv4 address, max. 19 characters `[0-9]`

**Default:**

any

### *2.20.248.1.11.3 Source-Port*

Specify the source port here.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**
4 characters `[0-9]`

**Default:**
0

### *2.20.248.1.11.4 Destination-Address*

Specify the destination IP address here.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**
IPv4 address, max. 19 characters `[0-9]`

**Default:**
any

### *2.20.248.1.11.5 Destination-Port*

Specify the destination port here.

**Telnet path:**
**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**
4 characters `[0-9]`

**Default:**

0

### *2.20.248.1.11.6 Protocol*

Here you specify the protocol used by the firewall.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

**Any**

ICMP, TCP and UDP

**ICMP**

**UDP**

**TCP**

**Default:**

Any

### *2.20.248.1.11.7 Additional-Parameters*

No current function.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

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

**Default:**

*empty*

### *2.20.248.1.11.8 Action*

Specify the frame handling here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

**Accept**

Accepted frames

**Drop**

Discards frames silent

**Reject**

Discards frames loud

**Default:**

Drop

### *2.20.248.1.11.9 Log*

Enable or disable the log here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

**No**

Log off

**Yes**

Log on

**Default:**

No

### *2.20.248.1.11.10 Trap*

Enable or disable traps here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

**No**

Traps off

**Yes**

Traps on

**Default:**

No

### *2.20.248.1.11.11 Status*

Specify the status of the firewall rule here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Table**

**Possible values:**

**1** Active
**2** Not-in-service
**3** Not-ready
**4** Create-and-go
**5** Create-and-wait
**6** Destroy

**Default:**

**2** Not-in-service

### 2.20.248.1.12 Rule-Mapping-Table

Here is the rule mapping table.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config**

#### *2.20.248.1.12.1 Rule-Index*

Specify the rule index here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

4 characters `[0-9]`

**Default:**

*empty*

#### *2.20.248.1.12.2 Associated-Bridge*

Here you specify to which bridge group the rule applies.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

**Selection from available bridge groups**

### *2.20.248.1.12.3 Priority*

Specify the rule priority here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

4 characters `[0-9]`

**Default:**

0

### *2.20.248.1.12.4 Direction*

Specify the direction of a rule here.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

**Ingress**
**Egress**
**Both**

**Default:**

Both

### *2.20.248.1.12.5 Interface-Index*

Here you specify the interfaces to which the rule should apply.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

**Selection from available interfaces**

### *2.20.248.1.12.6 Status*

Specify the status of the firewall mapping rule here.

**Telnet path:**

> **Setup** > **LAN-Bridge** > **L2-Firewall** > **Config** > **Rule-Mapping-Table**

**Possible values:**

**1**

Firewall mapping rule on

**2**

Firewall mapping rule off

**6**

Delete firewall mapping rule

**Default:**

1
2

## 2.20.248.2 Action

At this point you can execute actions for the L2 Firewall.

**Telnet path:**

> **Setup** > **LAN-Bridge** > **L2-Firewall**

#### 2.20.248.2.1 Reset-statistics

Reset the L2 Firewall statistics with this command.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Action**

**Possible arguments:**

*none*

#### 2.20.248.2.2 Flush-Tables

Close the connections previously opened in the L2 Firewall with this command.

**Telnet path:**

**Setup** > **LAN-Bridge** > **L2-Firewall** > **Action**

**Possible arguments:**

*none*

## 2.21 HTTP

This menu contains the HTTP settings.

**SNMP ID:** 2.21

**Telnet path:** /Setup

### 2.21.1 Document root

This parameter defines the path to a directory where the help for WEBconfig is stored locally.

**SNMP ID:** 2.21.1

**Telnet path:** /Setup/HTTP/Document-Root

**Possible values:**

- Maximum 99 alphanumerical characters

**Default:** Blank

**Note:** This parameter is for the future, local storage of WEBconfig help. This parameter has no function in current firmware versions.

## 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.

**SNMP ID:** 2.21.2

**Telnet path:** /Setup/HTTP

**Possible values:**

- Images
- Texts

**Default:** Images

**Note:** 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.

## 2.21.3 Font-Family

Font family for Web interface display.

**SNMP ID:** 2.21.3

**Telnet path:** /Setup/HTTP

**Possible values:**

- Max. 39 characters

**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.

**Telnet path:**/Setup/HTTP/Page-Headers

**Possible values:**

- Images
- Texts

**Default:** Images

### 2.21.6 Error-Page-Style

Normal error display or bluescreen

**SNMP ID:** 2.21.6

**Telnet path:** /Setup/HTTP

**Possible values:**

- Standard
- Nifty

### 2.21.7 Port

Port for the HTTP server connection

**SNMP ID:** 2.21.7

**Telnet path:** /Setup/HTTP

**Possible values:**

- Max. 5 characters

**Default:** 80

### 2.21.9 Max-Tunnel-Connections

The maximum number of simultaneously active HTTP tunnels

**SNMP ID:** 2.21.9

**Telnet path:** /Setup/HTTP

**Possible values:**

- Max. 255 tunnels

**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.

**SNMP ID:** 2.21.10

**Telnet path:** /Setup/HTTP

**Possible values:**

- Max. 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.

**SNMP ID:** 2.21.11

**Telnet path:** /Setup/HTTP

**Possible values:**

- Max. 10 characters

**Default:** 600

### 2.21.13 Standard-Design

Selects the design that will be used by default to display WEBconfig.

**SNMP ID:** 2.21.13

**Telnet 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.

**SNMP ID:** 2.21.14

**Telnet path:** /Setup/HTTP

#### 2.21.14.1 Device-information

Selection of device information to be displayed in WEBconfig.

**Telnet 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**
**DSLoL**

### 2.21.14.2 Position

Index for the sequence for the display of device information.

**Telnet path:**/Setup/HTTP/Show-device-information

**Possible values:**

- Max. 10 characters

**Default:** 0

## 2.21.15 HTTP-Compression

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.

**SNMP ID:** 2.21.15

**Telnet path:** /Setup/HTTP

**Possible values:**

- Activated
- Deactivated
- Only_for_WAN

**Default:** Activated

## 2.21.16 Keep-Server-Ports-Open

This menu contains the parameters for restricting access to the web server services.

**Telnet path:**/Setup/HTTP/Keep-Server-Ports-Open

## 2.21.16.1 Ifc.

Here you select the access path to be set for accessing the web-server services.

**Telnet path:**/Setup/HTTP/Keep-Server-Ports-Open/Ifc.

**Possible values:**

- All access methods provided by the device (e.g. LAN, WAN, WLAN, depending on the model).

**Default:** Blank

## 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.

**Telnet path:**/Setup/HTTP/Keep-Server-Ports-Open/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.
- Operating: 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.

**Default:** Automatic

### 2.21.20 Rollout-Wizard

This menu contains the settings for the Rollout Wizard.

**SNMP ID:** 2.21.20

**Telnet path:** /Setup/HTTP

## 2.21.20.1 Enabled

Switches the Rollout Wizard on or off. After being switched on the Wizard appears as an option on the WEBconfig start page.

**Telnet 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**.

**Telnet path:**

**Setup** > **HTTP** > **Rollout-Wizard**

**Possible values:**

Any string, max. 50 characters from

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

**Default:**

Rollout

## 2.21.20.3 Variables

This table defines the variables for the Rollout Wizard.

**Telnet path:** /Setup/HTTP/Rollout-Wizard

### 2.21.20.3.1 Index

Index for the variable. The Rollout Wizard displays the variables in ascending order.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- 1 to 232 - 1

**Default:** 0

### 2.21.20.3.2 Identity

Unique identifier of variables that are referenced during the execution of actions. Identifiers are not required for fields that are not used by users to enter their data (e.g. label).

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.21.20.3.3 Title

Name of the variable as displayed by the WEBconfig Rollout Wizard in .

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.21.20.3.4 Type

Type of variable.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- Label: Text that is displayed to provide explanations of the other variables. Min.-Value and Max.-Value are of no further significance for these entries.
- Integer: Allows the entry of a positive integer number between 0 and 232 - 1. By entering the Min.-Value and Max.-Value, the range of entries can be limited. Also, a default value can be defined. This default value must be between the min. and max. values.
- String: Enables text to be entered. By entering the Min.-Value and Max.-Value, the length of the string can be limited. Also, a default value can be defined. This default text must be shorter than the maximum length, otherwise it will be truncated.
- Password: splayed while being entered. Entering a password has to be repeated. The Rollout Wizard will execute no actions if the passwords do not agree.
- Checkmark: Simple option that can be switched on or off. Min.-Value and Max.-Value are of no further significance for these entries. Checkmarks are activated as standard if the default value is not empty.

**Default:** 0

### 2.21.20.3.5 Minimum value

Minimum value for the current variable (if type = integer) or minimum number of characters (where type = String or Password).

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- 0 to 232 - 1

**Default:** 0

#### 2.21.20.3.6 Maximum value

Maximum value for the current variable (if type = integer) or maximum number of characters (where type = String or Password).

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- 0 to 232 - 1

**Default:** 0

#### 2.21.20.3.7 Default value

Default value of the current variable.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Variables

**Possible values:**

- Max. 64 characters

**Default:** Blank

### 2.21.20.4 Actions

This table defines the actions for the Rollout Wizard.

**Telnet path:** /Setup/HTTP/Rollout-Wizard

#### 2.21.20.4.1 Index

Index for the action. The Rollout Wizard executes the actions in ascending order.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Actions

**Possible values:**

- 1 to 232 - 1

**Default:** 0

### 2.21.20.4.2 Action

Action to be executed by the Rollout Wizard after the user data have been entered.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Actions

**Possible values:**

- Similar to Cron commands, actions are entered in the syntax [Protocol:] Argument. If no protocol is entered, 'exec.' is applied.

**Default:** Blank

**Special values:** exec: Executes any command just as it is used in Telnet to configure a device. The following example sets the name of the device to 'MyDevice':

exec: set /setup/name MyDevice

mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:

mailto:admin@mycompany.com?subject=Rollout?body=Device setup completed

http and http: Enables a web site to be accessed, for example to carry out an action there.

<http:|https:>//[user[:pass]@]hostname[:port]/...

Variables in the actions: When actions are executed, the values as defined with the Rollout Wizard can be referenced. To this end, the variable's identifier is used for the action with a leading percent character. The identifier must be enclosed by curly brackets if other characters are included in the action. The following example sets the name of the device to the format 'Site (branch)', if the location of the device is being queried as a variable with the identifier 'Location':

exec: set /setup/name %{Location}(Filiale)

For variables of the type Integer or String, the value as entered by the user is used. In the case of variables of the type Checkmark, '1' (switched on) or '0' (switched off) is used.

**Note:** If the expression for the action contains spaces then the expression must be enclosed by quotation marks.

**Note:** To make use of the mail function, an SMTP account must be set up in the device.

#### 2.21.20.4.3 Description

Comment on the action.

**Telnet path:**/Setup/HTTP/Rollout-Wizard/Actions

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 2.21.20.5 Renumber variables

As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables/actions with neighboring index numbers require a new entry to be entered between them. With this action, the indices can automatically be renumbered with a certain interval between them.

When being executed, the arguments can be defined with the start value and increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

**Telnet path:** /Setup/HTTP/Rollout-Wizard

### 2.21.20.6 Renumber actions

As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables/actions with neighboring index numbers require a new entry to be entered between them. With this action,

the indices can automatically be renumbered with a certain interval between them.

When being executed, the arguments can be defined with the start value and increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

**Telnet path:** /Setup/HTTP/Rollout-Wizard

## 2.21.20.7 Display connection status

The first screen shows the status of the connection.

**Telnet path:** /Setup/HTTP/Rollout-Wizard

## 2.21.21 Max-HTTP-Job-Count

Using this setting you specify the maximum number of HTTPS jobs. An HTTP job exists when HiLCOS 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.

**Telnet path:**

**Setup** > **HTTP**

**Possible values:**

5 to 512

**Default:**

Depends on device

## 2.21.30 File-Server

This menu contains the file-server settings for external USB data media.

**SNMP ID:** 2.21.30

**Telnet path:** /Setup/HTTP/File-Server

### 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.

**Telnet path:**/Setup/HTTP/File-Server/Public-Subdir

**Possible values:**

- Maximum 64 alphanumerical characters

**Default:** public_html

### 2.21.30.2 Enabled

This parameter activates or deactivates the file server for USB media.

**Telnet path:**/Setup/HTTP/File-Server/Operating

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.21.40 SSL

The parameters for HTTPS connections are specified here.

**Telnet path:**
**Setup** > **HTTP**

### 2.21.40.3 Versions

This bitmask specifies which versions of the protocol are allowed.

**Telnet path:**
**Setup** > **HTTP** > **SSL**

**Possible values:**

**SSLv3**
**TLSv1**
**TLSv1.1**
**TLSv1.2**

**Default:**

SSLv3
TLSv1

## 2.21.40.4 Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

**Telnet 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.

**Telnet path:**

**Setup** > **HTTP** > **SSL**

**Possible values:**

**RC4-40**
**RC4-56**
**RC4-128**
**DES40**
**DES**
**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.

**Telnet 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.

**Telnet 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.

**Telnet 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

## 2.21.40.10 Port

Port for the HTTPS server connection

**Telnet 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.

**Telnet path:**
**Setup** > **HTTP** > **SSL**

**Possible values:**

**Yes**
**No**

**Default:**
Yes

# 2.22 SYSLOG

This menu contains the SYSLOG settings.

**SNMP ID:** 2.22

**Telnet path:** /Setup

## 2.22.1 Operating

Activates the dispatch of information about system events to the configured SYSLOG client.

**SNMP ID:** 2.22.1

**Telnet path:** /Setup/SYSLOG

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.22.2 SYSLOG table

This table defines the SYSLOG clients.

**SNMP ID:** 2.22.2

**Telnet path:** /Setup/SYSLOG

## 2.22.2.1 Idx.

Position of the entry in the table.

**SNMP ID:** 2.22.2.1

**Telnet path:** /Setup/SYSLOG/Server

**Possible values:**

- Max. 4 characters

**Default:** Blank

## 2.22.2.2 IP-Address

<IP address of the SYSLOG client>

**SNMP ID:** 2.22.2.2

**Telnet path:** /Setup/SYSLOG/Server

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

## 2.22.2.3 Source

Here you select which source is entered in the SYSLOG messages.

**Telnet 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.

**Telnet 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.

**SNMP ID:** 2.22.2.6

**Telnet path:** /Setup/SYSLOG/Server

**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

**Default:** Blank

### 2.22.3 Facility-Mapper

This table defines the allocation of SYSLOG sources to facilities.

**SNMP ID:** 2.22.3

**Telnet path:** /Setup/SYSLOG

## 2.22.3.1 Source

Mapping sources to specific facilities.

**SNMP ID:** 2.22.3.1

**Telnet 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.

**Telnet 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.

**SNMP ID:** 2.22.4

**Telnet path:** /Setup/SYSLOG

**Possible values:**

- Max. 10 characters

**Default:** 514

### 2.22.5 Messages-Table-Order

This item determines the order in which the messages table is displayed.

**SNMP ID:** 2.22.5

**Telnet path:** /Setup/SYSLOG

**Possible values:**

- Oldest on top
- Newest on top

**Default:** newest-on-top

### 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.

**Note:** This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

**SNMP ID:** 2.22.8

**Telnet path:** /Setup/SYSLOG

**Possible values:**

- Yes
- No

**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 *Remove old messages*.

**Telnet path:**

**Setup** > **SYSLOG**

**Possible values:**

1 to 99

**Default:**

24

### 2.22.10 Remove-Old-Messages

This parameter enables deletion of the SYSLOG messages in the device after the period set for *Maximum-message-age*.

**Telnet path:**

**Setup** > **SYSLOG**

**Possible values:**

Yes

No

**Default:**

No

### 2.22.11 Max-Age-Unit

This parameter determines whether the message age is specified in hours, days and months.

**Note:** In this case, a month is 30 days.

**Telnet 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.

**Telnet path:**
**Setup** > **SYSLOG**

**Possible values:**

**Emergency**
**Alert**
**Critical**
**Error**
**Warning**
**Notice**
**Info**
**Debug**

**Default:**
Critical

# 2.23 Interfaces

This menu contains the settings for the interfaces.

**SNMP ID:** 2.23

**Telnet path:** /Setup

## 2.23.4 DSL

The settings for the DSL interface are located here.

**SNMP ID:** 2.23.4

**Telnet path:** /Setup/Interfaces

### 2.23.4.1 Ifc

Specifies the interface that the settings refer to.

**SNMP ID:** 2.23.4.1

**Telnet path:** /Setup/Interfaces/S0/Ifc

**Possible values:**

- Choose from the DSL interfaces available in the device, e.g. DSL-1 or DSL-2.

**Note:** The selection options depend on the equipment of the device.

## 2.23.4.2 Operating

Here you can specify whether the interface is active or not.

**SNMP ID:** 2.23.4.2

**Telnet path:** /Setup/Interfaces/DSL/Operating

**Possible values:**

- No
- Yes

**Default:** No

## 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.

**Telnet path:**/Setup/Interfaces/DSL/Upstream-Rate

**Possible values:**

- Max. 6 numerical characters

**Default:** Blank

**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.

**Telnet path:**/Setup/Interfaces/DSL/Ext.-Overhead

**Possible values:**

- Max. 3 numerical characters

**Default:** Blank

### 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.

**Telnet path:**/Setup/Interfaces/DSL/Downstream-Rate

**Possible values:**

- Max. 6 numerical characters

**Default:** Blank

**Special values:** 0: No restriction on the received data traffic

## 2.23.7 Modem mobile

The settings for the mobile-telephony modem are located here.

**SNMP ID:** 2.23.7

**Telnet path:** /Setup/Interfaces

## 2.23.7.1 Ifc

Here you select the interface which you want to configure.

**Telnet path:**/Setup/Interfaces/Mobile/Ifc

**Possible values**:

- Modem

**Note:** The selection options depend on the equipment of the device.

## 2.23.7.2 Operating

Select the operating mode for the interface.

**Telnet path:**

**Setup** > **Interfaces** > **Modem-Mobile**

**Possible values:**

No

Modem

**Default:**

No

## 2.23.7.21 Data rate

Select the data rate in kilobytes per second used to transfer the data streams.

**Telnet path:**/Setup/Interfaces/Mobile/Datarate

**Possible Telnet values:**

- 19200
- 38400
- 57600
- 115200

**Default**: 115200

## 2.23.7.22 Profile

Here you select the profile to be used for the UMTS interface.

**Telnet path:**/Setup/Interfaces/Mobile/Profile

**Possible values:**

- Maximum 16 alphanumerical characters

**Default:** Blank

## 2.23.20 WLAN

This menu contains the settings for wireless LAN networks

**SNMP ID:** 2.23.20

**Telnet 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.

**SNMP ID:** 2.23.20.1

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.1.1 Ifc

Select from the logical WLAN interfaces.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- Select from the available logical WLAN interfaces.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- Max. 64 characters

**Default:** BLANK

### 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.

The option **Suppress SSID broadcast** provides the following settings:

- **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.

**Note:** 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.

#### Telnet path:

**Telnet path:Setup** > **Interfaces** > **WLAN** > **Network**

#### Possible values:

No

Yes

Tightened

**Default:**

No

### 2.23.20.1.8 Operating

Switches the logical WLAN on or off separately.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- On
- Off

**Default:** On

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- On
- Off

**Default:** On

**Note:** 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.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- 0 to 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.

**Note:** Client-bridge mode can only be used between two OpenBAT devices.

#### Telnet 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:**
Yes

### 2.23.20.1.12 RADIUS-Accounting

Deactivates accounting via a RADIUS server for this network

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- On
- Off

**Default:** Off

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- Yes
- No

**Default:** No

### 2.23.20.1.14 APSD

Activates APSD power saving for this logical WLAN network.

**Telnet path:**/Setup/Interfaces/WLAN/Network

**Possible values:**

- On
- Off

**Default:** Off

**Note:** 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.

### 2.23.20.1.15 Aironet-Extensions

Activates Aironet extensions for this logical wireless LAN.

**Telnet path:**/Setup/Interfaces/WLAN/Network/Aironet-Extensions

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.23.20.1.16Min-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.

#### Telnet path:

**Telnet 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.

**Telnet path:**

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

**Possible values:**

Yes

No

**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 or NetBIOS.

The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

**Telnet path:**

**Telnet path:Setup** > **Interfaces** > **WLAN** > **Network**

**Possible values:**

Yes

No

**Default:**

No

### 2.23.20.1.20 Summaric-Tx-Limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

**Possible values:**

0 … 4294967295 kbps

**Special values:**

**0**

This value disables the limit.

**Default:**

0

### 2.23.20.1.21 Summaric-Rx-Limit

With this setting, you define the overall bandwidth that is available for reception within this SSID.

**Telnet 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.

**Telnet 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 LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

**Telnet path:**

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

**Possible values:**

**No**

LBS tracking is disabled.

**Yes**

LBS tracking is enabled.

**Default:**

No

### 2.23.20.1.24 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.

**Telnet path:**

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

**Possible values:**

**Name** from **Setup** > **WLAN** > **Network** > **LBS-Tracking**

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

**Default:**

*empty*

### 2.23.20.1.248 Cl.-Brg.-Roaming-Support

Here you enable or disable the Client Bridge Roaming Support for the AP mode and the Client mode.

The Client Bridge Roaming Support improves the reliability and latency of the roaming process. It is useful in situations with many devices attached to the LAN of the Client and even more so, if most of the data traffic flows downstream; meaning, the traffic flows from the APs, through the Client to the attached devices. Enabling this feature on APs directly allows the APs to exchange information about the devices attached to a roaming Client. Enabling this feature on the Client allows freeing up the wireless link after roaming, which decreases roaming times. If this feature is enabled on the Client it will check on each roaming event if this improvement is possible or otherwise fall back on the default behavior.

**Telnet path:**

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

**Possible values:**

**No**

Client Bridge Roaming Support disabled

**Yes**

Client Bridge Roaming Support enabled

**Default:**

No

## 2.23.20.2 Transmission

Here you can adjust further transmission settings for each logical wireless LAN network (MultiSSID) supported by your device.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

### 2.23.20.2.1 Ifc

Opens the settings for the logical WLAN networks.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- Select from the available logical WLAN interfaces.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 500 to 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- Automatic
- Select from the available speeds

**Default:** Automatic

### 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Transmission**

**Possible values:**

Auto

Select from the available speeds of 1 Mbps – 54Mbps

**Default:**

2Mbps

#### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 512 to 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- On
- Off

**Default:** Off

#### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- Automatic
- Select from the available speeds

**Default:** Automatic

### 2.23.20.2.10 Min.-Frag.-Len

Packet fragment length below which fragments are dropped

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 0 to 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 0 to 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).

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Short-Guard-Interval

**Possible values:**

- Activated
- Disabled

**Default:** Activated

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Max.-Spatial-Streams

**Possible values:**

- Automatic
- One
- Two

**Default:** Automatic

### 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. .

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Send-Aggregates

**Possible values:**

- Yes
- No

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Min.-HT-MCS

**Possible values:**

- Automatic
- 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:** Automatic

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Max.-HT-MCS

**Possible values:**

- Automatic
- 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:** Automatic

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Min.-Spatial-Streams

**Possible values:**

- Automatic
- One
- Two

**Default:** Automatic

### 2.23.20.2.19 EAPOL-Rate

Set the data rate for EAPOL transmission here.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- Like-Data

Select from the available speeds:

- 1M
- 2M
- 5.5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-12M
- T-18M
- T-24M
- T-36M
- T-48M
- T-72M
- T-96M
- T-108M

**Default:** Like-Data

**Special values:** Like-Data transmits the EAPOL data at the same rate as payload 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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission/Max.-Aggr.-Packet-Number

**Possible values:**

- Max. 2 numerical characters

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Transmission

**Possible values:**

- 0 to 15

**Default:** 3

**Note:** Values larger than 15 are taken as 15.

### 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.

**Telnet 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).

**Note:** If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

#### Telnet path:

**Setup** > **Interfaces** > **WLAN** > **Transmission**

#### Possible values:

Yes

No

#### Default:

Yes (If the WLAN chipset supports STBC)

No (If the WLAN chipset does not support STBC)

### 2.23.20.2.24 Use-LDPC

Here you activate the use of LDPC for data transfer per logical network (SSID).

**Note:** If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

#### Telnet path:

**Setup** > **Interfaces** > **WLAN** > **Transmission**

#### Possible values:

Yes

No

#### Default:

Yes (If the WLAN chipset supports STBC)

No (If the WLAN chipset does not support STBC)

#### 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Transmission**

**Possible values:**

- None
- **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.

**Default:**

DHCP

### 2.23.20.3 Encryption

Here you can adjust the encryption settings for each logical wireless LAN network (MultiSSID).

**SNMP ID:** 2.23.20.3

**Telnet path:** /Setup/Interfaces/WLAN

#### 2.23.20.3.1 Ifc

Opens the WPA/WEP settings for the logical WLAN networks.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- Select from the available logical WLAN interfaces.

#### 2.23.20.3.2 Encryption

Activates the encryption for this logical WLAN.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- On
- Off

**Default:** On

### 2.23.20.3.3 Default key

Selects the WEP key to be used for encrypting packets sent by this logical WLAN.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- Key 1
- Key 2
- Key 3
- Key 4

**Default:** Key 1

**Note:** 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.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- 802-11i-(WPA)-PSK
- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)
- 802-11i-(WPA)-802.1x
- WEP-156 (128 bit)-802.1x

- WEP-128 (104 bit)-802.1x
- WEP-64 (40 bit)-802.1x

**Default:** WEP-128 (104 bit)

**Note:** Please consider that not all wireless cards support all encryption methods.

### 2.23.20.3.5 Authentication

The encryption method can be selected when using WEP.

**Telnet 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

**Note:** For reasons of security we recommend that you use the open system authentication procedure.

### 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'.

The following lengths result for the formats used:

Method, Length

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

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- ASCII character string or hexadecimal number

**Default:** Blank

**Note:** When using 802.1x in AP mode, the name entered here refers to the RADIUS server.

**Note:** When using 802.1x in client mode and PEAP or TTLS as the client EAP method, the credentials (user:password) are saved here.

### 2.23.20.3.9 WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- WPA1
- WPA2
- WPA1/2
- WPA2/3
- WPA3
- WPA1/2/3

**Default:** WPA2/3

### 2.23.20.3.10 Client-EAP-Method

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.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2

**Default:** TLS

**Note:** In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode.

### 2.23.20.3.11 WPA-Rekeying-Cycle

Defines how often a WPA key handshake will be retried during an existing connection (rekeying)

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- 0 to 4294967295 s

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- TKIP
- AES

- TKIP/AES

**Default:** TKIP

### 2.23.20.3.13 WPA2-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.

**Telnet path:**/Setup/Interfaces/WLAN/Encryption

**Possible values:**

- TKIP
- AES
- TKIP/AES

**Default:** AES

### 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.

**Telnet path:**

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

**Possible values:**

**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:**
Optional

### 2.23.20.3.15 PMK-Caching

Enables PMK caching in the WLAN client mode

**Telnet path:**

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

**Possible values:**

Yes

No

**Default:**

No

### 2.23.20.3.16Pre-Authentication

Enables pre-authentication support for the corresponding WLAN.

**Note:** In order to be able to use pre-authentication, PMK caching must be enabled.

**Telnet path:**

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

**Possible values:**

Yes
No

**Default:**

No

### 2.23.20.3.19 WPA2-Key-Management

You configure the WPA2 key management with these options.

**Important:** 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.

**Telnet path:**

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

**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 and Fast Roaming

#### 2.23.20.3.248 OKC

Turn OKC on or off here.

**Telnet path:**

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

**Possible values:**

**Yes**

OKC on

**No**

OKC off

**Default:**

No

### 2.23.20.4 Group-Encryption-Keys

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.

**SNMP ID:** 2.23.20.4

**Telnet path:** /Setup/Interfaces/WLAN

**Note:** 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.

#### 2.23.20.4.1 Ifc

Opens the WEP group keys for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 2.23.20.4.3 Key-2

WEP group key 2

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- 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

**Default:** Blank

### 2.23.20.4.4 Key-3

WEP group key 3

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- 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

**Default:** Blank

### 2.23.20.4.5 Key-4

WEP group key 4

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- You can enter the key as an ASCII character string or as a hexadecimal number (with a leading '0x')
- The following lengths result for the formats used:
- Method, Length
- 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

**Default:** Blank

### 2.23.20.4.7 Keytype-2

Select the key length to be used for the WEP group encryption key 2.

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

**Default:** WEP-64 (40 bit)

### 2.23.20.4.8 Keytype-3

Select the key length to be used for the WEP group encryption key 3.

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

**Default:** WEP-64 (40 bit)

### 2.23.20.4.9 Keytype-4

Select the key length to be used for the WEP group encryption key 4.

**Telnet path:**/Setup/Interfaces/WLAN/Group-Encryption-Keys

**Possible values:**

- WEP-156 (128 bit)
- WEP-128 (104 bit)
- WEP-64 (40 bit)

**Default:** WEP-64 (40 bit)

## 2.23.20.5 Interpoint-Settings

Here you can specify important parameters for the communication between and the behavior of base stations.

**SNMP ID:** 2.23.20.5

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.5.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 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".

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**Possible values:**

- Off: The access point only communicates with mobile clients
- On: The access point can communicate with other access points and with mobile clients
- Exclusive: The access point only communicates with other base stations

**Default:** Off

### 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 HiLCOS versions prior to version 2.70)

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**Possible values:**

- On
- Off

**Default:** Off

### 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.

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**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

**Note:** 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.

### 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.

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**Possible values:**

- 0 to 4294967295 seconds

**Default:** 4

### 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

**Telnet path:** /Setup/Interfaces/WLAN/Interpoint

**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.

**Telnet 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.

**Telnet 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.

**Telnet path:**
**Setup** > **Interfaces** > **WLAN** > **Interpoint-Settings**

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

**Default:**
*empty*

#### 2.23.20.5.248 C2C-Identifier

Specify the name for the C2C identifier here. The purpose of the C2C identifier in the context of C2C coupling is to identify potential P2P partners.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Settings**

**Possible values:**

Max. 24 characters from
`[A-Z][0-9][a-z]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

C2C_DEFAULT

### 2.23.20.6 Client-Settings

If you operate your device in client mode, you can make detailed settings on its behavior here.

**SNMP ID:** 2.23.20.6

**Telnet path:** /Setup/Interfaces/WLAN

#### 2.23.20.6.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- Selection from the available physical WLAN interfaces.

#### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- On
- Off

**Default:** On

### 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.

**Telnet 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.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- 2.4/5 GHz
- 2.4 GHz
- 5 GHz

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- Valid MAC address

**Default:** Blank

### 2.23.20.6.7 Address-Adaption

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.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- On
- Off

**Default:** Off

**Note:** Address adaptation only works when just one computer is connected to the client station.

### 2.23.20.6.12 Selection-Preference

Here you select the access point selection criteria of the client.

**Telnet path:**/Setup/Interfaces/WLAN/Client-Modes

**Possible values:**

- Signal strength: The priority of the access point will be defined in following order:
  - The access point with the greatest signal strength will be selected.
  - If 2 or more access points have the same signal strength, then the access point with the lowest channel utilization will be selected.
  - If the above parameters match for 2 or more access points, then the access point with the lowest index will be selected.

- Profile: The priority of the access point will be defined in following order:
  - The access point with the lowest index will be selected.
  - If matched profile defined at same index, then the access point with the lowest channel utilization will be selected.
  - If the above parameters match for 2 or more access points, then the access point with the highest signal strength will be selected.

- Channel Utilization:

The priority of the access point will be defined based on the parameters "Modem Channel Utilization" and "Number of station connected to AP". User have the option to choose if number of station connected to AP should be used for AP selection. This option can be enabled/disabled using the CLI command “/setup/wlan/ Selection-Preference-AP-Station”. Based on Channel Utilization information the access point will be selected in the following order:
- If the Selection-Preference-AP-Station parameter is enabled, the access point with the least stations connected to it will be selected.
- If station count of 2 or more access points is the same.Selects the profile for the WLAN offering lowest AP Channel Utilization
- If two or more Access point have same Channel Utilization and station count, then Access point offering the strongest signal will be selected.

**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.

**Telnet 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.

**SNMP ID:** 2.23.20.7

**Telnet path:** /Setup/Interfaces/WLAN

#### 2.23.20.7.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet 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.

**Telnet path:**/Setup/Interfaces/WLAN/Operational

**Possible values:**

- On
- Off

**Default:** On

### 2.23.20.7.3 Operation mode

Hirschmann devices can be operated in various operating modes:

**Telnet 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.

**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.

**Managed-AP:** As a managed access point, the device searches for a central WLAN Controller from which it can obtain a configuration.

**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 points:** Managed-AP

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Operational

**Possible values:**

- Number of connections: 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 signal 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.
- P2P1 to P2P6 signal 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:** Number of connections

### 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 HiLCOS 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 HiLCOS 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.

**Telnet path:**/Setup/Interfaces/WLAN/Operational/Broken-Link-Detection

**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

**Note:** 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.

**Note:** 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.

### 2.23.20.7.248 Assignment

Here you specify the WLAN interface usage in the client operating mode.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Operational**

**Possible values:**

**WLAN**

Standard connection (layer 2/layer 3) of the wired network.

**DSL-1**

Use the N:N mapping function over the WLAN interface.

**Default:**

WLAN

## 2.23.20.8 Radio-Settings

Here you can adjust settings that regulate the physical transmission and reception over your WLAN interface.

**SNMP ID:** 2.23.20.8

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.8.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 2.23.20.8.2 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- 0 to 999 dB

**Default:** 0

**Note:** 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.

#### 2.23.20.8.3 5GHz-Mode

Using two neighboring, vacant channels for wireless transmissions can increase the transfer speeds in Turbo Mode up to 108 Mbps.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Normal (54 Mbps mode)
- 108 Mbps (Turbo mode)

**Default:** Normal (802.11a) or 802.11a/n mixed (with 11n devices)

**Note:** This setting is only available for devices that support DFS2 or DFS3.

#### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- 0 to 65535 km

**Default:** 0

#### 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.

**Telnet 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Depends on the frequency band selected

**Default:** Band-1

### 2.23.20.8.8 Radio channel

The radio channel selects a portion of the conceivable frequency band for data transfer.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Depend on the selected frequency band and the selected country.

**Default:** 11

**Note:** In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

### 2.23.20.8.9 2.4GHz-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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- 802.11g/b mixed
- 802.11g/b 2-Mbit compatible
- 802.11b (11 Mbit)
- 802.11g (54 Mbit)
- 802.11g (108 Mbit)

**Default:** 802.11b/g mixed or 802.11b/g/n mixed (with 11n devices)

**Note:** 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.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Low
- Medium
- High
- Minicell
- Microcell

**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 O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:** Max. 4 characters

**Default:** 3

**Note:** The minimum of 6.5 dBm only applies to legacy abg radio modules with G-mode wireless LAN.

**Note:** 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'.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Comma-separated list of individual numbers or ranges.

**Default:** Blank

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- 0 to 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 750. 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.

**Note:** 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.

**Telnet 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.

**SNMP ID:** 2.23.20.8.17

**Telnet path:** /Setup/Interfaces/WLAN/Radio-Settings/Antenna-Mask

**Possible values:**

- Auto
- Antenna-1
- Antenna-1+2
- Antenna-1+3
- Antenna-1+2+3

**Default:** Auto

### 2.23.20.8.18 Background-Scan-Unit

Unit for the definition of the background scan interval

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings

**Possible values:**

- Milliseconds
- 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.

**Telnet path:**/Setup/Interfaces/WLAN/Radio-Settings/Channel-Pairing

**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.

**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.

**Note:** When upgrading a HiLCOS version to a current radio standard, the previous setting is retained.

**Telnet 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.

**Note:** 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Radio settings** > **CAC-Duration**

**Possible values:**

0 to 4294967295

**Default:**

60

### 2.23.20.8.22 Force-40MHz

Option forcing the device to use the 40-MHz bandwidth.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Radio settings** > **Force-40MHz**

**Possible values:**

Yes

No

**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**.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** 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 743 .

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Radio-settings**

**Possible values:**

0 … 4294967295

**Special values:**

**0**

For value '0' the best available free channel is automatically selected. If no free channel is available, a DFS scan will be performed first.

**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.

**Note:** 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Radio-settings**

**Possible values:**

**EN300328-V1.7**
**EN300328-V1.8**

**Default:**

EN300328-V1.8

### 2.23.20.8.248 Passive-Scan-Duration

Here you specify the duration in ms of the passive scan to a suitable value in accordance to the beacon interval of the APs.

This function allows you to adjust the duration of the passive scan to the beacon interval of the APs.

**Telnet path:**

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

**Possible values:**

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

**Default:**

400

## 2.23.20.9 Performance

Here you can set the parameters that influence the performance of your WLAN interface.

**SNMP ID:** 2.23.20.9

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.9.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Performance

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 2.23.20.9.2 Tx-Bursting

Enables/prevents packet bursting for increasing throughput. Bursting leads to less fairness on the medium.

**Telnet path:**/Setup/Interfaces/WLAN/Performance

**Possible values:**

- On
- Off

**Default:** Off

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Performance

**Possible values:**

- On
- Off

**Default:** Off

**Note:** 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.

## 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.

**SNMP ID:** 2.23.20.10

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.10.1 Ifc

Opens the Expert settings for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Beaconing

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 2.23.20.10.2 Beacon-Period

This value defines the time interval in Kµs between beacon transmission (1 Kµs corresponds to 1024 microseconds and is a measurement unit of the

802.11 standard. 1 Kµs 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.

**Telnet path:**/Setup/Interfaces/WLAN/Beaconing

**Possible values:**

- 20 to 65535 TU

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Beaconing

**Possible values:**

- 1 to 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 Kµs, then the beacons will be sent to the three WLANs every 100 Kµs. Depending on the beacon order, the beacons are transmitted at times as follows

**Telnet path:**/Setup/Interfaces/WLAN/Beaconing

**Possible values:**

- Cyclic: In this mode the access point transmits the first beacon transmission at 0 Kµs to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 Kµs) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 Kµs) 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 Kµs, WLAN-1 only is sent; after 33.3 Kµs WLAN-2, after 66.6 Kµs 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 Kµs) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

**Default:** Cyclic

**Note:** 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.

## 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.

**SNMP ID:** 2.23.20.11

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.11.1 Ifc

Opens the Expert settings for the physical WLAN interface.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- Selection from the available physical WLAN interfaces.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**Default:** 4

**Note:** Values which are too small may cause the client to detect lost connections more often than necessary.

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**Default:** 15

**Note:** Other contexts require the value of signal strengths in dB. The following conversion applies:

64dB - 100%

32dB - 50%

0dB - 0%

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- On
- Off

**Default:** On

### 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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 99%

**Default:** 0

### 2.23.20.11.9 Min-Connect-Signal-Level

Similar to the connection threshold, but specified as absolute signal strength

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to -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

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to -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.

**Telnet path:**/Setup/Interfaces/WLAN/Roaming

**Possible values:**

- 0 to 4294967295 seconds
- Maximum 10 characters

**Default:**

- 0

### 2.23.20.11.248 Prioritized-Channel-Scan

Enable or disable the prioritized channel scan function for the device here. The function is defined when the WLAN interface is configured as Station (Client mode).

The prioritized channel scan function optimizes roaming by including previous roaming decisions. This is suitable for scenarios with recurring movements of the clients within the WLAN. The prioritized channel scan function selects channels where potential roaming candidates are most likely to be found. This results in accelerated roaming, reduced handover times, and less packet loss.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Roaming**

**Possible values:**

**No**

Prioritized channel scan disabled

**Yes**

Prioritized channel scan enabled

**Default:**
No

## 2.23.20.12 Interpoint-Peers

Here you enter the wireless base stations that are to be networked via the point-to-point connection.

**SNMP ID:** 2.23.20.12

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.12.1 Ifc

Opens settings for the point-to-point peers.

**Telnet path:** Setup/Interfaces/WLAN/Interpoint-Peers

**Possible values:**

- Select from the available point-to-point connections.

### 2.23.20.12.2 Recognize by

Here you select the characteristics to be used to identify the P2P peer.

**Telnet 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.
- 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 remote station.

**Telnet path:** Setup/Interfaces/WLAN/Interpoint-Peers

**Possible values:**

- Valid MAC address

**Default:** Blank

**Note:** If you work with detection by MAC address, enter the MAC address of the WLAN adapter here and not that of the device itself.

### 2.23.20.12.4 Peer-Name

Station name of the P2P remote station

**Telnet 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.

**Telnet path:** Setup/Interfaces/WLAN/Interpoint-Peers

**Possible values:**

- On
- Off

**Default:** Off

### 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. The value `0` disables the limit (unlimited bandwidth).

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Peers**

**Possible values:**

0 to 4294967295

**Default:**

0

### 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. The value `0` disables the limit (unlimited bandwidth).

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Peers**

**Possible values:**

0 to 4294967295

**Default:**

0

### 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.

**Telnet 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.

- The **Connect-Threshold** defines the beacon signal strength with which the remote site must be received in order to establish the point-to-point link.
- The **Connect-Hold-Threshold** defines 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.

**Note:** The **Connect-Hold-Threshold** must be lower than the **Connect-Threshold**. The value `0` disables the corresponding limits.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Peers**

**Possible values:**

0 to 255

**Default:**

0

### 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.

- The **Connect-Threshold** defines the beacon signal strength with which the remote site must be received in order to establish the point-to-point link.
- The **Connect-Hold-Threshold** defines 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.

**Note:** The **Connect-Hold-Threshold** must be lower than the **Connect-Threshold**. The value `0` disables the corresponding limits.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Peers**

**Possible values:**

0 to 255

**Default:**

0

### 2.23.20.12.248 C2C-Mode

Select the operating mode for the C2C coupling here.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Peers**

**Possible values:**

**Automatic**

The APs start searching for P2P partners automatically. P2P partners with same C2C identifier automatically establish a P2P link. If several

partners have same C2C identifier, the connection is established to the closest partner.

**Manual**

1) The APs start and stop the search for P2P partners via the CLI. This makes use of the C2C identifier stored in the configuration.

2) The APs start and stop the search for P2P partners via the serial C2C interface protocol. The commands are issued by a control unit that also assigns the C2C identifiers to the APs.

**Default:**

Automatic

## 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).

**SNMP ID:** 2.23.20.13

**Telnet path:** /Setup/Interfaces/WLAN

### 2.23.20.13.1 Ifc

Select the logical WLAN network (SSID) for which you want to edit the network alarm limits.

**SNMP ID:** 2.23.20.13.1

**Telnet path:** /Setup/Interfaces/WLAN/Network-Alarm-Limits

**Possible values:**

- Choose from the SSIDs available in the device, e.g. WLAN-1, WLAN-2, etc.

### 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. Setting this value to 0 deactivates the check.

**SNMP ID:** 2.23.20.13.2

**Telnet path:** /Setup/Interfaces/WLAN/Network-Alarm-Limits

**Possible values:**

- 3 numerical characters

**Default:** 0

### 2.23.20.13.3 Total-Retries

The threshold value for the total number of transmission retries for the corresponding SSID. Once the value is reached, an alert is issued. Setting this value to 0 deactivates the check.

**SNMP ID:** 2.23.20.13.3

**Telnet path:** /Setup/Interfaces/WLAN/Network-Alarm-Limits

**Possible values:**

- 4 numeric characters to specify the repetitions in per mille

**Default:** 0 per mille

### 2.23.20.13.4 Tx-Errors

The total number of lost packets for the corresponding SSID. Once the value is reached, an alert is issued. Setting this value to 0 deactivates the check.

**SNMP ID:** 2.23.20.13.4

**Telnet path:** /Setup/Interfaces/WLAN/Network-Alarm-Limits

**Possible values:**

- 4 numeric characters to specify the repetitions in per mille

**Default:** 0 per mille

## 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.

**Note:** The device cannot transmit or receive data in this mode.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

#### 2.23.20.15.1 Ifc

Opens the settings for the physical WLAN interface.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Probe-Settings**

**Possible values:**

Selection from the available physical WLAN interfaces.

#### 2.23.20.15.2 Radio bands

Here you can select which frequency bands should be analyzed by spectral scanning.

**Telnet 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.

**Note:** The spectral scan only takes this field into account when either '2.4GHz' or '2.4GHz/5GHz' is set in **Radio bands**.

**Telnet 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 continu-

ous 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Probe-Settings**

**Possible values:**

Max. 48 characters

from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**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.

**Note:** The spectral scan only takes this field into account when either '5GHz' or '2.4GHz/5GHz' is set in **Radio bands**.

**Telnet 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

Specify in this field the channel list for the spectral scan in the 5GHz frequency band. Individual channels are separated with commas.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Probe-Settings**

**Possible values:**

Max. 48 characters

from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Probe-Settings**

**Possible values:**

Max. 10 characters

from 0 to 9

**Default:**

250

## 2.23.20.19 Interpoint-transmission

This table contains the transmission settings for the individual P2P links.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

### 2.23.20.19.1 Ifc

Name of the logical P2P interface which you selected.

**Telnet 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.

**Telnet 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.

**Telnet 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 RTS 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.

**Important:** The RTS/CTS threshold value also has to be set in the WLAN client, as far as the driver and/or operating system allow this.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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**.

**Telnet 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 µs (default) to 0.4 µs (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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** If the WLAN chipset does not support STBC, you cannot set this parameter to **Yes**.

**Telnet 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.

**Note:** If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

**Telnet 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

### 2.23.20.20.1 Ifc

Name of the physical WLAN interface

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Important:** Please note that not every client (or their hardware) supports every encryption method.

**Telnet 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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Encryption**

**Possible values:**

**WPA1**
**WPA2**
**WPA1/2**

**Default:**

WPA1/2

### 2.23.20.20.11 WPA-Rekeying-Cycle

Enter at which intervals the device repeats the WPA key handshake.

For WPA1/2, authentication on a network is performed with a pre-shared key (PSK), which is part of a 128-bit individual key. The device (as authenticator) generates this key with a 48-bit initial vector (IV), which makes it difficult for attackers to calculate the WPA key. The repetition of the key that consists of the IV and WPA keys only occurs after $2^{48}$ data packets, which no WLAN will reach within a foreseeable time.

To prevent the (theoretical) repetition of the real key, the WPA allows for an automatic renegotiation of the key with the WLAN client (the supplicant) in regular intervals (rekeying). This prevents the repetition of the real key. By setting an individual cycle, you have the option of shortening the rekeying intervals.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Encryption**

**Possible values:**

0 … 4294967295 Seconds

**Special values:**

**0**

This value disables the preliminary negotiation of a new WPA key at the device. Rekeying can still be triggered by the supplicant.

**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.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Encryption**

**Possible values:**

**TKIP**
**AES**
**TKIP/AES**

**Default:**

TKIP

### 2.23.20.20.13 WPA2-Session-Keytypes

Select the method or methods that the device offers the remote station for generating the WPA session or group key for WPA2. The device can provide the Temporal Key Integrity Protocol (TKIP) method, the Advanced Encryption Standard (AES) method, or both.

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Interpoint-Encryption**

**Possible values:**

**TKIP**
**AES**
**TKIP/AES**

**Default:**

AES

### 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.

**Telnet 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.

**Important:** 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.

**Telnet 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

### 2.23.21 LAN-interfaces

This menu contains the settings for the LAN interfaces.

**SNMP ID:** 2.23.21

**Telnet path:** /Setup/Interfaces/LAN-Interfaces

## 2.23.21.1 Ifc

This is where you select the LAN interface to which the subsequent settings are to apply.

**SNMP ID:** 2.23.21.1

**Telnet path:** /Setup/Interfaces/LAN-Interfaces/Ifc

**Possible values:**

- Select from the available LAN interfaces.

## 2.23.21.7 Operating

Activate or deactivate the corresponding LAN interface here.

**SNMP ID:** 2.23.21.7

**Telnet path:** /Setup/Interfaces/LAN-Interfaces

**Possible values:**

- Yes
- No

**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

**Note:** 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. The value 0 means there is no limit.

**SNMP ID:** 2.23.21.9

**Telnet path:** /Setup/Interfaces/LAN-Interfaces

**Possible values:**

- Maximum 10 numerical characters

**Default:** 0

**Note:** This setting is only available for devices with a WLAN module.

## 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.

**SNMP ID:** 2.23.30

**Telnet path:** /Setup/Interfaces

### 2.23.30.1 Port

The name of the selected port.

**Telnet 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.

**Telnet 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 PrivateMode

Once private mode is activated, this switch port is unable to exchange data directly with the other switch ports.

**Telnet path:**/Setup/Interfaces/Ethernet-Ports

**Possible values:**

- Yes
- No

**Default:** No

## 2.23.30.4 Assignment

Here you select how this interface is to be used.

**Telnet 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.

**Default:** Depends on the particular interface or the hardware model.

## 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.

**Telnet 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 works very well

in most cases. In some cases it may be necessary to influence master-slave negotiation.

**Telnet path:**/Setup/Interfaces/Ethernet-Ports/Clock-Role

**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

## 2.23.30.9 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.

### Telnet 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).

**Note:** 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.

## 2.23.40 Modem

More commands and options used for an optional external modem connected to the serial interface.

**SNMP ID:** 2.23.40

**Telnet path:** /Setup/Interfaces

## 2.23.40.1 Ring-Count

Number of rings before answering.

**Telnet path:**/Setup/Interfaces/Modem/Ring-Count

**Possible values:**

- Numerical characters from 0 to 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.

**Telnet path:**/Setup/Interfaces/Modem/Echo-Off-Command

**Possible values:**

- Maximum 9 alphanumerical characters

**Default:** E0

## 2.23.40.3 Reset

The device uses this command to perform a hardware reset on the externally connected modem.

**SNMP ID:** 2.23.40.3

**Telnet path:** /Setup/Interfaces/Modem/Reset

**Possible values:**

- Maximum 9 alphanumerical characters

**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.

**Telnet path:**/Setup/Interfaces/Modem/Init-Command

**Possible values:**

- Maximum 63 alphanumerical characters

**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.

**Telnet path:**/Setup/Interfaces/Modem/Dial-Command

**Possible values:**

- Maximum 31 alphanumerical characters

**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.

**Telnet path:**/Setup/Interfaces/Modem/Request-ID

**Possible values:**

- Maximum 9 alphanumerical characters

**Default:** I6

## 2.23.40.7 Accept calls

The device uses this command to accept a call arriving at the external modem.

**Telnet path:**/Setup/Interfaces/Modem/Answer-Command

**Possible values**:

- Max. 9 alphanumerical characters

**Default**: A

## 2.23.40.8 Disconnect command

The device uses this command to terminate calls made by the external modem (hang up).

**Telnet path:**/Setup/Interfaces/Modem/Disconnect-Command

**Possible values**:

- Max. 9 alphanumerical characters

**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.

**Telnet path:**/Setup/Interfaces/Modem/Escape-Sequence

**Possible values**:

- Max. 9 alphanumerical characters

**Default**: + + +

## 2.23.40.10 Escape prompt delay (ms)

After the escape sequence, the device waits for the time set here before issuing the command to hang up.

**Telnet path:**/Setup/Interfaces/Modem/Escape-Prompt-Delay-(ms)

**Possible values:**

- Numerical values from 0 to 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.

**Telnet path:**/Setup/Interfaces/Modem/Init.-Dial

**Possible values:**

- Maximum 63 alphanumerical characters

**Default:** Blank

## 2.23.40.12 Init.-Answer

The device sends the initialization sequence for answering to the external modem before outputting the accept-call command.

**Telnet path:**/Setup/Interfaces/Modem/Init.-Answer

**Possible values:**

- Maximum 63 alphanumerical characters

**Default:** Blank

## 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.

**Telnet path:**/Setup/Interfaces/Modem/Cycletime-AT-Poll-(s)

**Possible values:**

- Numerical characters from 0 to 9 seconds

**Default:** 1 second

## 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.

**Telnet path:**/Setup/Interfaces/Modem/AT-Poll-Count

**Possible values**

- Numerical characters from 0 to 9

**Default:** 5

### 2.23.41 Mobile

The settings for mobile telephony are located here.

**SNMP ID:** 2.23.41

**Telnet path:** /Setup/Interfaces/Mobile

## 2.23.41.1 Profiles

This table contains the settings for the GPRS/UMTS profiles.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles

#### 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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/Profile

**Possible values:**

- Maximum 16 alphanumerical characters

**Default:** Blank

#### 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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/PIN

**Possible values:**

- Max. 6 numerical characters

**Default:** Blank

**Note:** 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.

#### 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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/APN

**Possible values:**

- Maximum 48 alphanumerical characters

**Default:** Blank

#### 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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/Network

**Possible values:**

- Maximum 16 alphanumerical characters

**Default:** Blank

#### 2.23.41.1.5 Select

If you have opted for automatic mobile network selection, then the UMTS/GPRS interface will login to any available and valid mobile network. If you select manual mobile network selection, then the UMTS/GPRS interface will only login to the specified mobile network.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/Select

**Possible values:**

- Auto
- Manual

**Default:** Auto

**Note:** Manual selection of the mobile network is useful if the device is operated in a fixed location and the UMTS/GPRS interface should be prevented from logging into other networks, which may offer strong signals, but which may be undesirable or more expensive.

#### 2.23.41.1.6 Mode

Select the mobile networking transmission mode here.

#### Telnet 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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/QoS-Downstream-Datarate

**Possible values:**

- Max. 5 numerical characters

**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.

**Telnet path:**/Setup/Interfaces/Mobile/Profiles/QoS-Upstream-Datarate

**Possible values:**

- Max. 5 numerical characters

**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.

**Telnet path:**

**Setup** > **Interfaces** > **Mobile** > **Profiles**

**Possible values:**

IPv4

IPv6

IPv4v6

**Default:**

IPv4

### 2.23.41.1.10 LTE-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 following frequency bands are available:

- **B1_2100**: 2.1GHz band is enabled.
- **B3_1800**: 1.8GHz band is enabled.
- **B7_2600**: 2.6GHz band is enabled.
- **B8_900**: 900MHz band is enabled.
- **B20_800**: 800MHz band is enabled.
- **All**: All frequency bands are enabled.

**Note:** This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

**Telnet path:**

**Setup** > **Interfaces** > **Mobile** > **Profiles**

**Possible values:**

All

B1_2100

B3_1800

B7_2600

B8_900

B20_800

**Default:**

All

### 2.23.41.1.11 LTE-Attach

Here you specify whether the LTE attach takes place directly or after a time delay.

**Telnet path:**

**Setup** > **Interfaces** > **Mobile** > **Profiles**

**Possible values:**

**Immediate**
**Delayed**

**Default:**
Immediate

### 2.23.41.1.12 SIM-Slot

This parameter selects the SIM card slot that you want to link with the mobile profile.

**Telnet path:**
**Setup** > **Interfaces** > **Mobile** > **Profiles**

**Possible values:**

**0**
Profile inactive

**1**
SIM slot 1

**2**
SIM slot 2

**Default:**
0

## 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.

**Telnet path:**/Setup/Interfaces/Mobile/Scan-Networks

## 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.

**Telnet path:**/Setup/Interfaces/Mobile/Input-PUK

## 2.23.41.6 History interval (sec)

Logging interval in seconds for the values displayed for the modem status under History.

**Telnet path:** /Setup/Interfaces/Mobile/History-Interval(sec)

**Possible values:**

- 0 to 999999 seconds

**Default:** 0

**Special values:** '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.

**Telnet path:**/Setup/Interfaces/Mobile/Syslog-enabled

**Possible values:**

- Yes
- No

**Default:** No

## 2.23.41.8 Enable-HSUPA

HSUPA can be activated or deactivated here.

**Telnet path:**/Setup/Interfaces/Mobile/Enable-HSUPA

**Possible values:**

- Yes
- No

**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).

**Telnet path:**/Setup/Interfaces/Mobile/Signal-check-interval(min)

**Possible values:**

- 0 to 9999 minutes

**Default:** 0 minutes

**Special values:** '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.

**Telnet path:**/Setup/Interfaces/Mobile/Threshold-3G-to-2G[dB]

**Possible values:**

- -51 to -111 or 51 to 111 dB

**Default:** -89 dB

**Special values:** '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.

**Telnet path:**/Setup/Interfaces/Mobile/Check-while-connected

**Possible values:**

- Yes
- No

**Default:** Yes

**Note:** This setting only takes effect if the fallback from 3G to 2G connections has been configured.

### 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>
```

**Telnet path:**
**Setup** > **Interfaces** > **Mobile**

**Possible values:**
4 characters from `[0-9]`

## 2.24 Public-Spot-Module

This menu contains the settings for the Public Spot.

**SNMP ID:** 2.24

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Mode**

**Possible values:**

None

User+password

MAC+user+password

E-mail

E-Mail2SMS

Login-via-agreement

**Default:**

None

### 2.24.2 User-Table

Users who are to be granted access to your network are created as entries in the user table.

**SNMP ID:** 2.24.2

**Telnet path:** /Setup/Public-Spot-Module

#### 2.24.2.1 Name

Enter the user's name.

**Telnet path:**/Setup/Public-Spot-Module/User-Table/Name

**Possible values:**

- Max. 64 characters

### 2.24.2.2 Password

Enter a password.

**Telnet path:**/Setup/Public-Spot-Module/User-Table/Password

**Possible values:**

- Max. 16 characters

### 2.24.2.3 MAC-Address

Enter the MAC address here.

**Telnet path:**/Setup/Public-Spot-Module/User-Table/MAC-Address

**Possible values:**

- Max. 12 characters

### 2.24.2.4 Comment

You can enter a comment here.

**Telnet path:**/Setup/Public-Spot-Module/User-Table/Comment

**Possible values:**

- Max. 80 characters

### 2.24.2.5 Provider

Enter the provider's name.

**Telnet path:**/Setup/Public-Spot-Module/User-Table/Provider

**Possible values:**

- Max. 16 characters

### 2.24.2.6 Expiry

Enter the validity period for this setting (date).

**Telnet path:**/Setup/Public-Spot-Module/User-Table/Expiry

**Possible values:**

- Max. 20 characters

## 2.24.3 Provider-Table

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.

**SNMP ID:** 2.24.3

**Telnet path:** /Setup/Public-Spot-Module

**Note:** 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.

### 2.24.3.1 Name

Name of the RADIUS server provider who supplies the authentication and/or accounting.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Name

**Possible values:**

- Max. 16 alphanumerical characters

**Default:** Blank

### 2.24.3.3 Auth.-Server-Port

Enter here the port used by the server that the Public Spot requests for authenticating the access sessions with this provider.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Port

**Possible values:**

- Valid port name

**Default:** l0

### 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.

**SNMP ID:** 2.24.3.4

**Telnet path:** /Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Secret

**Possible values:**

- Max. 32 alphanumerical characters

**Default:** Blank

### 2.24.3.6 Acc.-Server-Port

Enter here the port used by the server that the Public Spot uses for the accounting of the access sessions with this provider.

**SNMP ID:** 2.24.3.6

**Telnet path:** /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Port

**Possible values:**

- Valid port name

**Default:** l0

### 2.24.3.7 Acc.-Server-Key

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.

**SNMP ID:** 2.24.3.7

**Telnet path:** /Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Secret

**Possible values:**

- Max. 32 alphanumerical characters

**Default:** Blank

## 2.24.3.8 Backup

From the provider table, select a different entry to be used as 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.

**SNMP ID:** 2.24.3.8

**Telnet path:** Setup/Public-Spot-Module/Provider-Table/Backup

**Possible values:**

- Selection from the list of defined RADIUS providers (max. 16 characters).

**Default:** Blank

## 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.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Loopback-Addr.

**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
- LBO ... LBF for the 16 loopback addresses
- Any valid IP address

**Default:** Blank

### 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.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Loopback-Addr.

**Possible values:**

**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
- LBO ... LBF for the 16 loopback addresses
- Any valid IP address

**Default:** Blank

### 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.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Auth.-Server-Protocol

**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.

**Telnet path:**/Setup/Public-Spot-Module/Provider-Table/Acc.-Server-Protocol

**Possible values:**

- RADIUS
- RADSEC

**Default:** RADIUS

## 2.24.3.13 Auth.-Server-Host-Name

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server which the Public Spot contacts for authentication with this provider.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Provider-Table**

**Possible values:**

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

**Default:**

*empty*

## 2.24.3.14 Acc.-Server-Host-Name

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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Provider-Table**

**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`.

**Telnet path:**
**Setup** > **Public-Spot-Module** > **Provider-Table** > **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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Provider-Table** > **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.

**SNMP ID:** 2.24.5

**Telnet path:** /Setup/Public-Spot-Module

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.24.6

**Telnet path:** /Setup/Public-Spot-Module/Server-Subdir

**Possible values**:

- Max. 127 characters

**Default:** Blank

### 2.24.7 Accounting cycle

Define the time in seconds for the accounting cycle.

**SNMP ID:** 2.24.7

**Telnet path:** /Setup/Public-Spot-Module

### 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.

**SNMP ID:** 2.24.8

**Telnet path:** /Setup/Public-Spot-Module

#### 2.24.8.1 Page

Name of the page that your customers can use without logging in.

**SNMP ID:** 2.24.8.1

**Telnet path:** /Setup/Public-Spot-Module/Page-Table/Page

#### 2.24.8.2 URL

URL of the page that your customers can use without logging in.

**SNMP ID:** 2.24.8.2

**Telnet path:** /Setup/Public-Spot-Module/Page-Table/URL

**Possible values:**

- Max. 100 characters

**Default:** By default, different HTML pages stored on the device file system can be displayed, depending on the page chosen by the user.

## 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.

**SNMP ID:** 2.24.8.3

**Telnet path:** /Setup/Public-Spot-Module/Page-Table/Fallback

**Possible values:**

- Yes
- No

**Default:** No

## 2.24.8.4 Type

Select the type of the page.

**SNMP ID:** 2.24.8.4

**Telnet path:** /Setup/Public-Spot-Module/Page-Table/Type

**Possible values:**

- Template
- Redirect

**Default:** Template

## 2.24.8.5 Loopback-Addr.

Enter a loopback address.

**SNMP ID:** 2.24.8.5

**Telnet path:** /Setup/Public-Spot-Module/Page-Table/Loopback-Addr.

**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

**Default:** Blank

### 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.

**SNMP ID:** 2.24.9

**Telnet path:** /Setup/Public-Spot-Module/Roaming-Secret

**Possible values**:

- Max. 32 characters

**Default:** Blank

### 2.24.12 Communication port

Here you set the port that the Public Spot uses to communicate with the clients associated with it.

**SNMP ID:** 2.24.12

**Telnet path:** /Setup/Public-Spot-Module/Communication-Port

**Possible values:**

- Any valid port descriptor, max. 5 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.24.14

**Telnet path:** /Setup/Public-Spot-Module

**Possible values**:

- Max. 10 characters

**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.

**SNMP ID:** 2.24.15

**Telnet path:** /Setup/Public-Spot-Module/Port-Table

## 2.24.15.2 Port

Select the port for which you want to activate or deactivate authentication by the Public Spot.

**SNMP ID:** 2.24.15.2

**Telnet path:** /Setup/Public-Spot-Module/Port-Table/Port

**Possible values:**

- Choose from the device's ports, e.g. LAN-1

## 2.24.15.3 Authentication-Necessary

Activate or deactivate authentication by the Public Spot for the selected port.

**SNMP ID:** 2.24.15.3

**Telnet path:** /Setup/Public-Spot-Module/Port-Table/Authentication-Necessary

**Possible values:**

- Yes
- No

**Default:** No

### 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.

**SNMP ID:** 2.24.16

**Telnet path:** /Setup/Public-Spot-Module

**Possible values:**

- Yes
- No

**Default:** No

### 2.24.17 Provide-Server-Database

Here you can select whether the Public Spot provides the MAC address list via RADIUS.

**SNMP ID:** 2.24.17

**Telnet path:** /Setup/Public-Spot-Module/Provide-Server-Database

**Possible values**:

- Yes
- No

**Default:** No

### 2.24.18 Disallow-Multiple-Login

Allows a single user account to login multiple times simultaneously.

**SNMP ID:** 2.24.18

**Telnet path:** /Setup/Public-Spot-Module

**Possible values:**

- No
- Yes

**Default:** No

**Note:** 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.

### 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.

**SNMP ID:** 2.24.19

**Telnet path:** /Setup/Public-Spot-Module

## 2.24.19.2 Username-Pattern

This item defines the format of the name of new user accounts.

**SNMP ID:** 2.24.19.2

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard

**Possible values:**

- Max. 19 characters The string '%n' is a placeholder for a unique account number that is automatically generated by the Public Spot.

**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.

**SNMP ID:** 2.24.19.3

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard

**Possible values:**

- 0 to 255

**Default:** 6

## 2.24.19.4 SSID

Enter the SSID that Public Spot Add-User wizard prints out on the form for the user.

**SNMP ID:** 2.24.19.4

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard

**English description**: SSID

**Possible values:**

- Max. 32 alphanumerical characters

**Default:** Blank

**Note:** If you leave this field blank, the Public Spot Add-User wizard fills out the form with the SSID of the first logical WLAN with an activated Public Spot.

## 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.

**SNMP ID:** 2.24.19.5

**Telnet 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.

**SNMP ID:** 2.24.19.5.1

**Telnet path:** /Setup/Public-Spot-Module/Default-Runtime

**Possible values:** Max. 5 characters

**Default:** Blank

#### 2.24.19.5.2 Unit

Select the unit to be used for the runtime of a user account on the Public Spot.

**SNMP ID:** 2.24.19.5.2

**Telnet path:** /Setup/Public-Spot-Module/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.

**SNMP ID:** 2.24.19.6

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard/Comment-Fields

#### 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.

**Telnet path:** /Setup/Public-Spot-Module/Add-User-Wizard/Comment-Fields/Field-Name

**Possible values:**

- Max. 31 characters

**Default:** Blank

**Note:** Activate the printout of the comments with the option *2.24.19.8 Print-Comments-On-Voucher.*

### 2.24.19.7 Default-Starting-Time

Here you select the starting time at which the voucher's runtime begins. By using the option to commence the runtime at the first login, you can print out a supply of vouchers in advance. The user can still use the full runtime.

**SNMP ID:** 2.24.19.7

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard/Default-Starting-Time

Specify the default starting time here.

**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.

**SNMP ID:** 2.24.19.8

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard/Print-Comments-on-Voucher

**Possible values:**

- Yes
- No

**Default:** No

## 2.24.19.9 Maximal-Voucher-Validity-Period

This value defines the maximum validity period of the voucher in days.

**SNMP ID:** 2.24.19.9

**Telnet path:** Setup/Public-Spot-Module/Add-User-Wizard/Maximal-Voucher-Validity-Period

**Possible values:**

- Max. 10 characters

**Default:** 365 days

**Note:** If you starting time for the voucher's runtime to 'first login' (*2.24.19.7 Default starting time*), 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.

## 2.24.19.10Available-expiry-methods

Use this setting to determine which expiry methods are offered by the Public-Spot add-user wizard when creating new user accounts.

**SNMP ID:** 2.24.19.10

**Telnet path:** /Setup/Public-Spot-Module/Add-User-Wizard/Available-expiry-methods

**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.

**Default:** All methods

**Note:** If you select the login-time 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 Maximum-Voucher-Validity-Period*).

## 2.24.19.11 SSID-Table

This table contains the list of network names available for Public Spot users.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **SSID-Table**

### 2.24.19.11.1 Network name

Enter here the name of a logical WLAN (stored in the device) for which access is to be provided to Public Spot users by means of billable vouchers.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **SSID-Table**

**Possible values:**

Maximum 32 alphanumerical characters

from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default**

Blank

#### 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **SSID-Table**

**Possible values:**

No

Yes

**Default**

No

### 2.24.19.12 Case-sensitive

This setting specifies whether the name of the newly created Public Spot user is handled case-sensitive.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.24.19.14Max-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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **Max-Concurrent-Logins-Table**

**Possible values:**

Max. 5 numbers

**Default:**

0, 3, 10

**Special values:**

0 enables an unlimited number of logins for a single account.

### 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".

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **Max-Concurrent-Logins-Table**

**Possible values:**

0 to 99999

**Default:**

## 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.

**Telnet 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**.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard**

### 2.24.19.17.1 Profile name

Enter the name for the bandwidth profile here.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

**Possible values:**

String, max. 255 characters

**Default:**

### 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`.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

**Possible values:**

0 to 4294967295

**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`.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Add-User-Wizard** > **Bandwidth-profiles**

**Possible values:**

0 to 4294967295

**Default:**

0

### 2.24.19.18 Password input set

This setting specifies the character set used by the **Create Public Spot Account** wizard to create passwords for new users.

**Telnet 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.

**Telnet 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.

**Telnet 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

## 2.24.20 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.

**SNMP ID:** 2.24.20

**Telnet path:** /Setup/Public-Spot-Module

### 2.24.20.1 VLAN-ID

Enter the VLAN ID here.

**Telnet path:** /Setup/Public-Spot-Module/Add-User-Wizard/VLAN-Table/VLAN-ID

**Possible values:**

- 0 to 4096

**Default:** Blank

## 2.24.21 Login-Page-Type

Here you select the protocol to be used by the Public Spot to display the login pages.

**SNMP ID:** 2.24.21

**Telnet path:** /Setup/Public-Spot-Module/Login-Page-Type

**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.

**SNMP ID:** 2.24.22

**Telnet path:** /Setup/Public-Spot-Module

**Possible values:**

- Max. 31 characters

**Default:** Blank

### 2.24.23 MAC-Address-Table

This table contains the WLAN clients that can automatically authenticate to the Public Spot using the MAC address.

**Telnet path:**

**Setup** > **Public-Spot**

## 2.24.23.1 MAC-Address

MAC address of the WLAN client that can use automatic authentication.

**Telnet path:**

**Setup** > **Public-Spot** > **MAC-Address-Table**

**Possible values:**

Valid MAC address, 12 characters

**Default:**

## 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.

**Telnet path:**

**Setup** > **Public-Spot** > **MAC-Address-Table**

**Possible values:**

A name that is unique within this table; maximum 32 alphanumeric characters

**Default:**

## 2.24.23.3 Provider

The Public Spot takes this provider for the optional session accounting by means of RADIUS server.

**Telnet path:**

**Setup** > **Public-Spot** > **MAC-Address-Table**

**Possible values:**

One of the RADIUS servers defined in the provider list.

**Default:**

## 2.24.24 MAC-Address-Check-Provider

The Public Spot uses this provider to authenticate the MAC address by means of RADIUS server.

**Note:** 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.

**Telnet path:**

**Setup** > **Public-Spot** >

**Possible values:**

One of the RADIUS servers defined in the provider list.

**Default:**

## 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.

**Telnet path:**

**Setup** > **Public-Spot**

**Possible values:**

0 to 4294967295

**Default:**

60

## 2.24.26 Station-Table-Limit

You can increase the maximum number of clients up to 65,536.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Station-Table-Limit**

**Possible values:**

16 to 65536

**Default:**

8192

**Note:** 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.

## 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.

**SNMP ID:** 2.24.30

**Telnet path:** /Setup/Public-Spot-Module/Free-Server

**Possible values**:

- Max. 64 characters

**Default:** Blank

## 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 HiLCOS version 8.80 you also have the option to enter the hostname using wildcards.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Free-Networks**

### 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.

#### Telnet path:

**Setup** > **Public-Spot-Module** > **Free-Networks** > **Host-Name**

#### Possible values:

Max. 64 Characters, including letters, numbers, hyphens, periods (.), and wildcards (?, *).

#### Default:

Blank

### 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.

#### Telnet path:

**Setup** > **Public-Spot-Module** > **Free-Networks** > **Mask**

#### Possible values:

Max. 15 characters

#### 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.

**Telnet 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").

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Free-Hosts-Minimum-TTL**

**Possible values:**

Max. 10 characters

**Special values:**

0: The validity period is set by the duration in the DNS response (TTL).

**Default:**

300

## 2.24.33 Login-Text

The setting allows you to specify a custom text that the device inserts into the box on the login form of the Public Spot module's authentication page. 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:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das
Formular aus.</i>)
```

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Possible values:**

Any string, max. 254 characters from

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

**Default:**

## 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.

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Possible values:**

Valid name of a remote station, max. 16 characters

**Default:**

## 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 Hirschmann". 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.

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Possible values:**

No

Yes

**Default:**

Yes

## 2.24.36User-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

**Note:** Remember to upload a page with the terms and conditions onto the device before you require them to be confirmed.

**Telnet 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.

**Note:** 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`.

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Possible values:**

No

Yes

**Default:**

Yes

## 2.24.40 XML-Interface

Configure the XML interface here.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **XML-Interface**

### 2.24.40.1 Operating

Enable the XML interface here.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **XML-Interface**

**Possible values:**

Yes

No

**Default:**

No

### 2.24.40.2Radius-Authentication

This item enables or disables authentication by a RADIUS server when using the XML interface of the Public Spot.

**Note:** The additional authentication by RADIUS server is only active if the Public Spot's XML interface is enabled (see *XML interface)*.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **XML-Interface**

**Possible values:**

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.

No: No additional authentication necessary

**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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules**

## 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Limit-e-mails-per-Hour**

**Possible values:**

Max. 5 numbers

**Default:**

100

#### 2.24.41.1.3 Subject

Enter the subject line of the e-mail that is sent.

The subject line may also contain the following control characters:

- `\n`: CRLF (carriage return, line feed)
- `\t`: Tabulator

- \xy: ASCII code of the corresponding character

**Note:** You can use these control characters in the subject line, as well as in the text content for e-mail or e-mail2SMS. If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents HiLCOS from modifying the "\".

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Subject**

**Possible values:**

Max. 250 characters

**Default:**

Your Public Spot Account

#### 2.24.41.1.4 Body

With this parameter you can specify the contents of the e-mail, where "$PSpotPasswd" is the variable for the generated password.

The body text may also contain the following control characters:

- \n: CRLF (carriage return, line feed)
- \t: Tabulator
- \xy: ASCII code of the corresponding character

**Note:** You can use these control characters in the subject line, as well as in the text content for e-mail or e-mail2SMS. If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents HiLCOS from modifying the "\".

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Body**

**Possible values:**

Max. 500 characters

**Default:**

Your Public Spot login credentials: User name: <Your e-mail address> Password: $PSpotPasswd $PSpotLogoutLink

### 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Max-Request-Attempts**

**Possible values:**

Max. 5 numbers

**Default:**

3

### 2.24.41.1.6 Local-e-mail-Address

Enter the sender e-mail address for the e-mail that is sent.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Local-e-mail-Address**

**Possible values:**

Valid e-mail address with a maximum of 150 characters.

**Default:**

Blank

### 2.24.41.1.7 Name

Enter the sender name for the e-mail that is sent.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Real-Name**

**Possible values:**

Max. 150 characters

**Default:**

Blank

### 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.

**Telnet 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 *Black-White-Domain-List* you determine whether you accept or reject a provider.

**Important:** Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

**Possible values:**

Valid e-mail domains (such as @hotmail.com) with a maximum of 150 characters.

**Default:**

Blank

#### *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 *Black-White-Domain-List* you determine whether you accept or reject a provider.

**Important:** Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Domain-List**

**Possible values:**

Valid e-mail domains (such as @hotmail.com) with a maximum of 150 characters.

**Default:**

Blank

### 2.24.41.1.20 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Real-Name**

#### *2.24.41.1.20.2 Content*

Use this parameter to set the sender name used for the selected language.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Real-Name**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

### 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication**

#### *2.24.41.1.21.1 Language*

This parameter shows the language variant for the individual message text.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Body**

### *2.24.41.1.21.2 Content*

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

**Note:** 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 HiLCOS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Body**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Subject**

#### *2.24.41.1.22.2 Content*

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

**Note:** 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 HiLCOS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Subject**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

## 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication** > **Limit-e-mails-per-Hour**

**Possible values:**

Max. 5 numbers

**Default:**

100

#### 2.24.41.2.3 Subject

Enter the subject line of the e-mail that is sent. Keep in mind any formatting specifications for the SMS gateway.

The subject line may also contain the following control characters:

- `\n`: CRLF (carriage return, line feed)
- `\t`: Tabulator
- `\xy`: ASCII code of the corresponding character

**Note:** You can use these control characters in the subject line, as well as in the text content for e-mail or e-mail2SMS. If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents HiLCOS from modifying the "\".

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PSpotUserMobileNr` for the user's mobile phone number
- `$PSpotPasswd` for the user's password generated by the Public Spot

**Note:** The Public Spot transmits the user's mobile phone number set with the variable `$PSpotUserMobileNr` without any leading zeros to the SMS gateway. If the SMS gateway expects a certain string for the country code (e.g. "00" or "+"), then enter this prefix in front of the variable.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Subject**

**Possible values:**

Max. 250 characters

**Default:**

Your Public Spot login credentials.

#### 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Max-Request-Attempts**

**Possible values:**

Max. 5 numbers

**Default:**

3

#### 2.24.41.2.5 Local-e-mail-Address

Enter the sender e-mail address for the e-mail that is sent.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Local-e-mail-Address**

**Possible values:**

Max. 150 characters

**Default:**

Blank

#### 2.24.41.2.6 Name

Enter the sender name of the SMS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Real-Name**

**Possible values:**

Max. 150 characters

**Default:**

Blank

### 2.24.41.2.12 Body

This parameter sets the contents of the sent e-mail. Keep in mind any formatting specifications for the SMS gateway.

The body text may also contain the following control characters:

- `\n`: CRLF (carriage return, line feed)
- `\t`: Tabulator
- `\xy`: ASCII code of the corresponding character

**Note:** You can use these control characters in the subject line, as well as in the text content for e-mail or e-mail2SMS. If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents HiLCOS from modifying the "\".

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PSpotUserMobileNr` for the user's mobile phone number
- `$PSpotPasswd` for the user's password generated by the Public Spot

**Note:** The Public Spot transmits the user's mobile phone number set with the variable `$PSpotUserMobileNr` without any leading zeros to the SMS gateway. If the SMS gateway expects a certain string for the country code (e.g. "00" or "+"), then enter this prefix in front of the variable.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Body**

**Possible values:**

Max. 512 characters

**Default:**

#Key#Route#From#

### 2.24.41.2.13 Gateway-E-Mail-Address

Here you enter the 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

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail-Authentication** > **Gateway-e-mail-Address**

**Possible values:**

Valid e-mail address of the gateway with maximum 150 characters. .

**Default:**

Blank

### 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.

**Telnet 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`.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Allowed-Country-Codes**

**Possible values:**

String, max. 150 characters

**Default:**

#### *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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Allowed-Country-Codes**

**Possible values:**

Any valid country code, max. 5 characters

**Default:**

0

### 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.

**Important:** SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

**Important:** In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Setup** > **Mail**.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

**Possible values:**

**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.

**Note:** 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 username

With this parameter you specify the user name used by your device to authenticate at another device.

**Telnet 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.

**Telnet 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.

**Telnet 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*

### 2.24.41.2.23 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-

mail2SMS. If you do not specify any text for a language, the device automatically enters the internal default text.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication**

### *2.24.41.1.22.1 Language*

This parameter shows the language variant for the individual sender name.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Real-Name**

### *2.24.41.2.23.2 Content*

Use this parameter to set the sender name used for the selected language.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Real-Name**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Body**

#### *2.24.41.2.24.2 Content*

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

**Note:** 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 HiLCOS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Body**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Subject**

#### *2.24.41.2.25.2 Content*

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

**Note:** 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 HiLCOS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2SMS-Authentication** > **Subject**

**Possible values:**

Any string, max. 251 characters from

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

**Default:**

## 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**.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

String, max. 251 characters

**Default:**

### 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.

**Telnet 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. The value `0` deactivates the function.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 4294967295

**Default:**

0

#### 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 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.

**Telnet 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".

**Important:** In order for this setting to work, the parameter ***Multiple-Login*** must be enabled.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 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 ***Max-concurrent-logins***.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

Yes

No

**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. The value `0` disables the limit (unlimited bandwidth).

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 4294967295

**Default:**

0

### 2.24.41.3.11 Rx-Limit

With this setting you limit the maximum receiving bandwidth (in kbps), which is available to the user. The value `0` disables the limit (unlimited bandwidth).

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **User-Template**

**Possible values:**

0 to 4294967295

**Default:**

0

## 2.24.41.4Login-via-agreement

In this menu, you specify the settings for automatic login and authentication via RADIUS.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules**

### 2.24.41.4.1Max-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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

**Possible values:**

0 to 65535

**Default:**

100

### 2.24.41.4.2User-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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

**Possible values:**

0 to 65535

**Default:**

1

#### 2.24.41.4.3Username-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).

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

**Possible values:**

String, max. 10 characters

**Default:**

free

### 2.24.42 WISPr

This menu contains the WISPr settings.

**Telnet path:**

**Setup** > **Public-Spot-Module**

## 2.24.42.1 Enabled

Enable or disable the WISPr function for your device.

**Telnet 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>`

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

String, max. 255 characters, with the following restrictions:

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

**Default:**

## 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

String, max. 255 characters, with the following restrictions:

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

**Default:**

## 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

String, max. 255 characters, with the following restrictions:

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

**Default:**

## 2.24.42.5 Login-URL

Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

HTTPS URL, max. 255 characters

**Default:**

## 2.24.42.6 Logout-URL

Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

HTTPS URL, max. 255 characters

**Default:**

### 2.24.42.7 Disconnect login URL

Enter the HTTPS address to which the device forwards a WISPr client if authentication fails.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

HTTPS URL, max. 255 characters

**Default:**

### 2.24.42.8 Max-Authen-Failure

Enter the maximum number of failed attempts which the login page of your Internet service provider allows.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **WISPr**

**Possible values:**

0 to 65535

**Default:**

5

## 2.24.43 Advertisement

This menu gives you the option to enable or disable advertising pop-ups, and to edit these.

**Telnet path:**

**Setup** > **Public-Spot-Module**

## 2.24.43.1 Operating

This menu switches the advertisements on or off.

**Telnet 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.

**Telnet 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.

**Telnet 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).

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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

## 2.24.47 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.

**Note:** 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) .

### Telnet 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.

**Note:** To learn more about the request and response types, as well as the `SOURCE_VLAN` element, refer to the User Guide.

### 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”.

**Telnet path:**

**Setup** > **Public Spot**

## 2.24.48.1 Administrator

Contains the name of the administrator who is entitled to assign this circuit ID.

**Telnet 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.

**Telnet path:**

**Setup** > **Public-Spot** > **Circuit-IDs**

**Possible values:**

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

**Default:**

*empty*

### 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.

**Note:** 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.

**Telnet path:**

**Setup** > **Public-Spot-Module**

## 2.24.50.1 Operating

Enable or disable the automatic re-login with this action.

**Note:** 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Auto-Re-Login**

**Possible values:**

Yes

No

**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.

**Note:** 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.

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Auto-Re-Login**

**Possible values:**

16 to 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.

**Note:** 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".

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Auto-Re-Login**

**Possible values:**

Max. 10 characters

**Default:**

259200

## 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).

**Telnet path:**

**Setup** > **Public-Spot-Module**

## 2.24.60.1 Language

This parameter shows the language of the login text to be entered.

**Telnet 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>)
```

**Telnet path:**
**Setup** > **Public-Spot-Module** > **Login-Text**

**Possible values:**

Any string, max. 254 characters from

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

**Default:**

## 2.25 RADIUS

This menu contains the settings for the RADIUS server.

**SNMP ID:** 2.25

**Telnet path:** /Setup

### 2.25.4 Auth.-Timeout

This value specifies how many milliseconds should elapse before retrying RADIUS authentication.

**SNMP ID:** 2.25.4

**Telnet path:** /Setup/RADIUS

**Possible values:**

- Max. 10 characters

**Default:** 5000

### 2.25.5 Auth.-Retry

This value specifies how many authentication attempts are made in total before a Reject is issued.

**SNMP ID:** 2.25.5

**Telnet path:** /Setup/RADIUS

**Possible values:**

- Max. 10 characters

**Default:** 3

### 2.25.9 Backup-Query-Strategy

This value specifies how the device should handle unanswered queries from multiple RADIUS servers.

**SNMP ID:** 2.25.9

**Telnet path:** /Setup/RADIUS/Backup-Query-Strategy

**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.

**SNMP ID:** 2.25.10

**Telnet 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.

**SNMP ID:** 2.25.10.1

**Telnet path:** /Setup/RADIUS/Server

**Possible values:**

- Max. 5 numbers

**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.

**Telnet 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.

**SNMP ID:** 2.25.10.2.1

**Telnet path:** /Setup/RADIUS/Server/Clients

**Possible values:**

- Valid IP address

**Default:** Blank

### 2.25.10.2.2 Secret

Password required by the client for access to the RADIUS server in the access point.

**SNMP ID:** 2.25.10.2.2

**Telnet path:** /Setup/RADIUS/Server/Clients

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.25.10.2.3 IP-Netmask

IP netmask of the RADIUS client

**SNMP ID:** 2.25.10.2.3

**Telnet path:** /Setup/RADIUS/Server/Clients

**Possible values:**

- Valid IP address

**Default:** Blank

### 2.25.10.2.4 Protocols

Protocol for communication between the internal RADIUS server and the clients.

**SNMP ID:** 2.25.10.2.4

**Telnet path:** /Setup/RADIUS/Server/Clients

**Possible values:**

- RADSEC
- RADIUS
- all

**Default:** RADIUS

### 2.25.10.2.5 Comment

Comment on this entry.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Clients**

**Possible values:**

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

**Default:**

*empty*

## 2.25.10.3 Forward-Servers

If you wish to use RADIUS forwarding, you have to specify further settings here.

**SNMP ID:** 2.25.10.3

**Telnet path:** /Setup/RADIUS/Server

### 2.25.10.3.1 Realm

String with which the RADIUS server identifies the forwarding destination.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

Max. 64 characters

**Default:**

Blank

### 2.25.10.3.3 Port

Open port for communications with the forwarding server.

**SNMP ID:** 2.25.10.3.3

**Telnet path:** /Setup/RADIUS/Server/Forward-Servers

**Possible values:**

- Max. 10 characters

**Default:** 0

### 2.25.10.3.4 Secret

Password required for accessing the forwarding server.

**SNMP ID:** 2.25.10.3.4

**Telnet path:** /Setup/RADIUS/Server/Forward-Servers

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.25.10.3.5 Backup

Alternative routing server that the RADIUS server forwards requests to when the first routing server is not reachable.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

Max. 64 characters

**Default:**

Blank

### 2.25.10.3.6 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.

**SNMP ID:** 2.25.10.3.6

**Telnet path:** /Setup/RADIUS/Server/Forward-Servers

**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

**Default:** Blank

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

### 2.25.10.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

**SNMP ID:** 2.25.10.3.7

**Telnet 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

0 to 65535

**Default:**

0

### 2.25.10.3.10 Accnt.-Secret

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that in the accounting server.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

Any key, max. 64 characters

**Default:**

### 2.25.10.3.11 Accnt.-Loopback-Address

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.

**Telnet 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

  **Note:** 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

**Note:** If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

**Default:**

### 2.25.10.3.10 Accnt.-Protocol

Using this item you specify the protocol that the forwarding accounting server uses.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

RADIUS

RADSEC

**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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet 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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet 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`.

**Telnet 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`.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

### 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.

**Telnet path:**

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

**Possible values:**

Max. 64 characters

**Default:**

Blank

### 2.25.10.6 Empty-Realm

This realm is used when the specified username does not contain a realm.

**Telnet path:**

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

**Possible values:**

Max. 64 characters

**Default:**

Blank

## 2.25.10.7 User name

In the following table, enter the data for the users that are to be authenticated by this server.

**SNMP ID:** 2.25.10.7

**Telnet path:** /Setup/RADIUS/Server/Users

**Multiple logins**

Allows a single user account to login multiple times simultaneously.

Possible values: Yes, No

Default: Yes

**Note:** 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.

**Expiry type**

This option defines how the validity period is limited for a user account.

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.

Default: Blank: The user account never expires, unless a predefined time or volume budget expires.

**Note:** The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

**Note:** The device must have a valid time in order for the device to work with user-account time budgets.

**Abs.-Expiry**

If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined by this value.

Possible values: Valid time information (date and time). Max. 20 characters from 0123456789/:.Pp

Default: Blank

Special values: 0 switches off the monitoring of the absolute expiry time.

**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.

Possible values: Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the relative expiry time.

**Time budget**

The maximum duration of access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

Possible values: Time span in seconds. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of the time budget.

**Volume budget**

The maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

Possible values: Volume budget in Bytes. Max. 10 characters from 0123456789

Default: 0

Special values: 0 switches off the monitoring of data volume.

**Comment**

Comment on this entry.

**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.

Possible values:

- 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.
- Any

Default: Any

**Note:** 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.

### 2.25.10.7.1 User name

User name.

**SNMP ID:** 2.25.10.7.1

**Telnet path:** /Setup/RADIUS/Server/Users

**Possible values:**

- Max. 48 characters

**Default:** Blank

### 2.25.10.7.2 Password

User password.

**SNMP ID:** 2.25.10.7.2

**Telnet path:** /Setup/RADIUS/Server/Users

**Possible values:**

- Max. 32 characters

**Default:** Blank

### 2.25.10.7.3 Limited-Auth-Methods

This option allows you to place limitations on the authentication methods permitted for the user.

**SNMP ID:** 2.25.10.7.3

**Telnet path:** /Setup/RADIUS/Server/Users

**Possible values:**

- Any combination of the following 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.

**Note:** 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`.

**Note:** 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

0 to 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`).

**Telnet 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`).

**Telnet 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.

**Telnet path:**/Setup/RADIUS/Server/Users/Tx-Limit

**Possible values:**

- 0 to 4294967295 (2^32-1)

**Default:** 0

#### 2.25.10.7.8 Rx-Limit

Limitation of bandwidth for RADIUS clients.

**Telnet path:**/Setup/RADIUS/Server/Users/Rx-Limit

**Possible values:**

- 0 to 4294967295 (2^32-1)

**Default:** 0

#### 2.25.10.7.9 Multiple-Login

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.

**Telnet path:**/Setup/RADIUS/Server/Users/Multiple-Login

**Possible values:**

- Yes
- No

**Default:** Yes

**Note:** 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.

### 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.

**SNMP ID:** 2.25.10.7.10

**Telnet path:** /Setup/RADIUS/Server/Users/Abs.-Expiry

**Possible values:**

- Valid time information (date and time). Max. 20 characters from 0123456789/:.

**Default:** 0

**Special values:** 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. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

**SNMP ID:** 2.25.10.7.11

**Telnet path:** /Setup/RADIUS/Server/Users/Time-Budget

**Possible values:**

- Time span in seconds. Max. 10 characters from 0123456789

**Default:** 0

**Special values:** 0 switches off the monitoring of the time budget.

### 2.25.10.7.13 Expiry-Type

This option defines how the validity period is limited for a user account.

**Telnet path:**/Setup/RADIUS/Server/Forward servers/Expiry-Type

**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

**Note:** The two options can be combined. In this case the user account expires when one of the two limiting values has been reached.

**Note:** The device must have a valid time in order for the device to work with user-account time budgets.

### 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.

**SNMP ID:** 2.25.10.7.14

**Telnet path:** /Setup/RADIUS/Server/Users/Rel.-Expiry

**Possible values:**

- Time span in seconds. Max. 10 characters from 0123456789

**Default:** 0

**Special values:** 0 switches off the monitoring of the relative expiry time.

### 2.25.10.7.15 Comment

Comment on this entry.

**SNMP ID:** 2.25.10.7.15

**Telnet path:** HiLCOS Menu Tree/Setup/RADIUS/Server/Users/

Comment **Possible values:**

- Max. 64 characters

**Default:** Blank

### 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'.

**SNMP ID:** 2.25.10.7.16

**Telnet path:** /Setup/RADIUS/Server/Users/Service-Type

**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

**Note:** 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.

### 2.25.10.7.17 Case-Sensitive

This setting specifies whether the RADIUS server handles the user name case-sensitive.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.25.10.7.18 WPA-Passphrase

Here you can specify the WPA passphrase with which users can login to the WLAN.

**Note:** 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).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

8 to 63 characters from the ASCII character set

**Default:**

### 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

0 to 4294967295

**Default:**

0

### 2.25.10.7.20 Active

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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

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

**Default:**

0

**Special values:**

**0**

The volume budget is deactivated.

### 2.25.10.10 EAP

This menu contains the EAP settings.

**SNMP ID:** 2.25.10.10

**Telnet 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.

**SNMP ID:** 2.25.10.10.1

**Telnet path:** /Setup/RADIUS/Server/EAP

**Possible values:**

- Max. 24 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.25.10.10.3

**Telnet path:** /Setup/RADIUS/Server/EAP

**Possible values:**

- Max. 10 numbers

**Default:** 0

**Special values:** 0: No timeout is sent to the authenticator.

**Note:** 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.

**SNMP ID:** 2.25.10.10.4

**Telnet path:** /Setup/RADIUS/Server/EAP

**Possible values:**

- Max. 10 numbers

**Default:** 0

**Special values:** 0: No timeout is sent to the authenticator.

**Note:** 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.

**SNMP ID:** 2.25.10.10.5

**Telnet 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.

**SNMP ID:** 2.25.10.10.6

**Telnet 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.

**SNMP ID:** 2.25.10.10.7

**Telnet path:** /Setup/RADIUS/Server/EAP

**Possible values:**

- None
- MD5
- GTC
- MSCHAPv2
- TLS
- TTLS
- PEAP

**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.

**SNMP ID:** 2.25.10.10.8

**Telnet path:** /Setup/RADIUS/Server/EAP/Default-MTU

**Possible values:**

- 100 to 1496 bytes

**Default:** 1036 bytes

### 2.25.10.10.9 Allow-Methods

Here you select the server and the method for the EAP authentication.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **Allow-Methods**

#### *2.25.10.10.9.1 Method*

Select the default EAP authentication method.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **Allow-Methods**

**Possible values:**

MD5

GTC

MSCHAPv2

TLS

TTLS

PEAP

**Default:**

MD5

#### *2.25.10.10.9.2 Allow EAP-TLS*

Enable the EAP-TLS method for authentication here.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **Allow-Methods**

**Possible values:**

On

Off

Internal only

**Default:**

On

### 2.25.10.10.10MSCHAPv2-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:** Note that the external RADIUS server must support at least MSCHAPv2 because CHAP leaves the actual password on the server.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP**

**Possible values:**

Valid DNS name or IP address of the server. Value range:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
```

**Default:**

Blank

### 2.25.10.10.18 EAP-SIM

802.11u networks make it possible for WLAN clients in the area of coverage to automatically log in to the provider's hotspot with the login data of the provider's own SIM card.

In this directory you specify the SIM access credentials for automatic authentication.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP**

### *2.25.10.10.18.1 Card-Keys*

Using this table you configure the SIM cards for automatic authentication with EAP SIM.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM**

#### 2.25.10.10.18.1.1 User name

Enter the user name for the EAP-SIM authentication here. With EAP-SIM, the username consists of

- a leading 1,
- the mobile country code (MCC),
- the mobile network code (MNC),
- the international mobile subscriber identity (IMSI) and
- the @realm

. This results in the following syntax:

```
Syntax:   1<MCC><MNC><IMSI>@<Realm> Example:
1262011234567890@wlan.mnc001.mcc262.3gppnetwork.org
```

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 48 characters from
`[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.# `

**Default:**

*empty*

### 2.25.10.10.18.1.5 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`).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**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*

### 2.25.10.10.18.1.6 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`).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**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*

### 2.25.10.10.18.1.7 Rand1

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 32 characters from `0123456789abcdef`

**Default:**

00000000000000000000000000000000

#### 2.25.10.10.18.1.8 SRES1

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 8 characters from `0123456789abcdef`

**Default:**

00000000

#### 2.25.10.10.18.1.9 Kc1

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 16 characters from `0123456789abcdef`

**Default:**

0000000000000000

#### 2.25.10.10.18.1.10 Rand2

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-

bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 32 characters from `0123456789abcdef`

**Default:**

00000000000000000000000000000000

#### 2.25.10.10.18.1.11 SRES2

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 8 characters from `0123456789abcdef`

**Default:**

00000000

#### 2.25.10.10.18.1.12 Kc2

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 16 characters from `0123456789abcdef`

**Default:**

0000000000000000

### 2.25.10.10.18.1.13 Rand3

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 32 characters from `0123456789abcdef`

**Default:**

00000000000000000000000000000000

### 2.25.10.10.18.1.11 SRES3

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 8 characters from `0123456789abcdef`

**Default:**

00000000

#### 2.25.10.10.18.1.15 Kc3

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

**Possible values:**

Max. 16 characters from `0123456789abcdef`

**Default:**

0000000000000000

### 2.25.10.10.19 EAP-TLS

The parameters for EAP-TLS connections are specified here.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP**

#### *2.25.10.10.19.3 Key-exchange algorithms*

This bitmask specifies which key-exchange methods are available.

**Telnet 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.

**Telnet path:**
**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

**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

### *2.25.10.10.19.5 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.

**Telnet 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

**Possible values:**

**On**
**Off**

**Default:**
On

### *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.

**Telnet path:**
**Setup** > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

**Possible values:**

**Yes**
**No**

**Default:**
No

## 2.25.10.11 Accounting-Port

Enter the port used by the RADIUS server to receive accounting information. Port '1813' is normally used.

**SNMP ID:** 2.25.10.11

**Telnet path:** /Setup/RADIUS/Server

**Possible values:**

- Max. 4 numbers

**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.

**SNMP ID:** 2.25.10.12

**Telnet path:** /Setup/RADIUS/Server

**Possible values:**

- Max. 4 numbers

**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.

**SNMP ID:** 2.25.10.13

**Telnet path:** /Setup/RADIUS/Server

**Possible values:**

- Max. 5 numbers

**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.

**Telnet path:**/Setup/RADIUS/Server/Auto-Cleanup-User-Table

**Possible values:**

- Yes
- No

**Default:** No

## 2.25.10.15 Allow-Status-Requests

Here you specify whether to allow status requests.

**SNMP ID:** 2.25.10.15

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **IPv6-Clients**

**Possible values:**

**RADIUS**
**RADSEC**
**All**

**Default:**
RADIUS

### 2.25.10.16.5 Comment

Comment on this entry.

**Telnet path:**
**Setup** > **RADIUS** > **Server** > **IPv6-Clients**

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

**Default:**
*empty*

## 2.25.10.17 Realm types

Specify how the RADIUS server determines the realm of a RADIUS request.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

**No**

Accouting information is not automatically deleted.

**Yes**

Accounting information is deleted automatically.

**Default:**

No

## 2.25.20 RADSEC

The parameters for READSEC connections are specified here.

**Telnet path:**

**Setup** > **RADIUS**

## 2.25.20.1 Versions

This bitmask specifies which versions of the protocol are allowed.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **RADIUS** > **RADSEC**

**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

## 2.25.20.4 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.

**Telnet 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.

**Telnet 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.

**Telnet 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

## 2.26 NTP

This menu contains the NTP settings.

**SNMP ID:** 2.26

**Telnet path:** /Setup

### 2.26.2 Server-Operating

Here you switch on the time server in your device for the local network. Other devices in the same network can then synchronize with the server via the network time protocol (NTP).

**SNMP ID:** 2.26.2

**Telnet path:** /Setup/NTP

**Possible values:**

- Yes
- No

**Default:** No

## 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.

**Note:** The send mode of the device only supports IPv4 addresses.

**Telnet 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.

**SNMP ID:** 2.26.4

**Telnet path:** /Setup/NTP

**Possible values:**

- Max. 10 characters

**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).

**SNMP ID:** 2.26.7

**Telnet path:** /Setup/NTP

**Possible values:**

- Max. 10 characters

**Default:** 86400

**Note:** A connection may be established in order to access the time server. Please be aware that this may give rise to additional costs.

### 2.26.11 RQ-Address

Here you enter the time server that supplies the correct current time.

**SNMP ID:** 2.26.11

**Telnet 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.

**Telnet 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.

**Note:** 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

**Telnet path:**
**Setup** > **NTP** > **RQ-Address**

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

**Default:**
*empty*

### 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.

**SNMP ID:** 2.26.12

**Telnet path:** /Setup/NTP

**Possible values:**

- Max. 10 characters

**Default:** 4

## 2.27 Mail

This menu contains the e-mail settings.

**SNMP ID:** 2.27

**Telnet 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.

**SNMP ID:** 2.27.1

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 31 characters

**Default:** Blank

**Note:** A connection may be established in order to send e-mail messages. Please be aware that this may give rise to additional costs.

## 2.27.2 Serverport

Enter the number of the SMTP port of the aforementioned server for unencrypted e-mail transmission. The default value is 587.

**Telnet path:**

**Setup** > **Mail**

**Possible values:**

Max. 10 characters

**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".

**SNMP ID:** 2.27.3

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 31 characters

**Default:** Blank

## 2.27.4 POP3-Port

Enter the number of the POP3 port of the aforementioned server for unencrypted mail. The default value is 110.

**SNMP ID:** 2.27.4

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.27.5

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 63 characters

**Default:** Blank

### 2.27.6 Password

Enter the password to be used to send e-mail notifications to the aforementioned SMTP server.

**SNMP ID:** 2.27.6

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 31 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.27.7

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 63 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.27.8

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.27.9

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.27.10

**Telnet path:** /Setup/Mail

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.27.11

**Telnet path:** /Setup/Mail

**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

**Default:** Blank

**Note:** If there is an interface called "DMZ", its name will be taken in this case.

## 2.27.12 SMTP-use-TLS

Here you determine if and how the device encrypts the connection. The available values have the following meanings:

- **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. This setting is the default value.
- **Required**: Connection establishment is not encrypted. If the SMTP server does not offer STARTTLS, the device does not transmits any data.

**Telnet path:**

**Setup** > **Mail**

**Possible values:**

No

Yes

Preferred

Required

**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:

**Telnet 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

# 2.30 IEEE802.1x

This menu contains the settings for the IEEE802.1x protocol.

**SNMP ID:** 2.30

**Telnet path:** /Setup

## 2.30.3 Radius-Server

Authentication in all wireless LAN networks by a central RADIUS server (named DEFAULT) can be managed here. You can also define RADIUS servers that are dedicated to certain wireless LAN networks (instead of defining the passphrase for the logical wireless LAN network). Furthermore, a backup server can be specified for every RADIUS server.

**SNMP ID:** 2.30.3

**Telnet path:** /Setup/IEEE802.1x

### 2.30.3.1 Name

The name of the server.

**SNMP ID:** 2.30.3.1

**Telnet path:** /Setup/IEEE802.1x /RADIUS-Server

**Possible values:**

- Max. 16 characters

**Default:** Blank

## 2.30.3.3 Port

The port the RADIUS server.

**SNMP ID:** 2.30.3.3

**Telnet path:** /Setup/IEEE802.1x /RADIUS-Server

**Possible values:**

- Max. 10 characters

**Default:** 0

## 2.30.3.4 Secret

The secret used by the RADIUS server.

**SNMP ID:** 2.30.3.4

**Telnet path:** /Setup/IEEE802.1x /RADIUS-Server

**Possible values:**

- Max. 32 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.30.3.5

**Telnet path:** /Setup/IEEE802.1x /RADIUS-Server

**Possible values:**

- Max. 24 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.30.3.6

**Telnet path:** /Setup/IEEE802.1x /RADIUS-Server

**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

**Note:** 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

## 2.30.3.7 Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

**SNMP ID:** 2.30.3.7

**Telnet path:** /Setup/IEEE802.1x/RADIUS-Server/Protocol

**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.

**Note:** The RADIUS client automatically detects which address type is involved.

**Telnet path:**

**Setup** > **IEEE802.1x** > **RADIUS-Server**

**Possible values:**

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

**Default:**

*empty*

**Special values:**

**DEFAULT**

The name "DEFAULT" is reserved for all WLAN networks that use IEEE 802.1x for authentication and that do not have their own RADIUS server. Every WLAN that uses authentication by IEEE 802.1x can use its own RADIUS server after specifying appropriate values for 'Key1/Passphrase'.

### 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`.

**Telnet path:**

**Setup** > **IEEE802.1x** > **RADIUS-Server**

**Possible values:**

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

**Default:**

*empty*

### 2.30.4 Ports

You should specify the login settings separately for each local network.

**SNMP ID:** 2.30.4

**Telnet path:** /Setup/IEEE802.1x

## 2.30.4.2 Port

The interface that this entry refers to.

**SNMP ID:** 2.30.4.2

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- All of the interfaces available in the device.

**Default:** Blank

## 2.30.4.4 Re-Auth-Max

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.4

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 3

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

## 2.30.4.5 Max-Req

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.5

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 3

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

## 2.30.4.6 Tx-Period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.6

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 30

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

### 2.30.4.7 Supp-Timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.7

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 30

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

### 2.30.4.8 Server-Timeout

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.8

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 30

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

### 2.30.4.9 Quiet-Period

This parameter is a timer in the authentication state machine for IEEE 802.1x.

**SNMP ID:** 2.30.4.9

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 60

**Note:** Changes to these parameters require expert knowledge of the IEEE 802.1x standard. Only make changes here if your system configuration absolutely requires them.

## 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.

**SNMP ID:** 2.30.4.10

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Yes
- No

**Default:** No

## 2.30.4.11 Re-Auth-Interval

A typical value as a re-authentication interval is 3,600 seconds.

**SNMP ID:** 2.30.4.11

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 3600

### 2.30.4.12 Key-Transmission

Here you activate the regular generation and transmission of a dynamic WEP key.

**SNMP ID:** 2.30.4.12

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Yes
- No

**Default:** No

### 2.30.4.13 Key-Tx-Interval

A typical value as a key-transmission interval is 900 seconds.

**SNMP ID:** 2.30.4.13

**Telnet path:** /Setup/IEEE802.1x /Ports

**Possible values:**

- Max. 10 characters

**Default:** 900

## 2.31 PPPoE-Server

This menu contains the settings for the PPPoE server.

**Telnet path:**
**Setup**

## 2.31.1 Operating

This switch enables and disables the PPPoE server.

**SNMP ID:** 2.31.1

**Telnet path:** /Setup/PPPoE-Server

**Possible values:**

- Yes
- 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.

**SNMP ID:** 2.31.2

**Telnet path:** /Setup/PPPoE-Server

## 2.31.2.1 Peer

Here you can define a remote-station name for each client. The remote-site name must be used by the client as the PPP user name.

**SNMP ID:** 2.31.2.1

**Telnet path:** /Setup/PPPoE-Server/Name-List

**Possible values:**

- Select from the list of defined peers.

**Default:** Blank

## 2.31.2.2 SH-Time

Define the short-hold time for the PPPoE connection here.

**SNMP ID:** 2.31.2.2

**Telnet path:** /Setup/PPPoE-Server/Name-List

**Possible values:**

- Max. 10 characters

**Default:** 0

### 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.

**SNMP ID:** 2.31.2.3

**Telnet path:** /Setup/PPPoE-Server/Name-List

**Possible values:**

- Max. 12 characters

**Default:** 000000000000

## 2.31.3 Service

The name of the service offered is entered under 'Service'. his enables a PPPoE client to select a certain PPPoE server that is entered for the client.

**SNMP ID:** 2.31.3

**Telnet path:** /Setup/PPPoE-Server

**Possible values:**

- Max. 32 characters

**Default:** Blank

## 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.

**SNMP ID:** 2.31.4

**Telnet path:** /Setup/PPPoE-Server

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.31.5

**Telnet path:** /Setup/PPPoE-Server

### 2.31.5.2 Port

Port for which the PPPoE server is to be activated/deactivated.

**SNMP ID:** 2.31.5.2

**Telnet path:** /Setup/PPPoE-Server/Ports

**Possible values:**

- Selects a port from the list of those available in the device.

### 2.31.5.3 Enable PPPoE

Activates or deactivates the PPPoE server for the selected port.

**SNMP ID:** 2.31.5.3

**Telnet path:** /Setup/PPPoE-Server/Ports

**Possible values:**

- Yes
- No

**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).

**Telnet 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*

## 2.32 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

**SNMP ID:** 2.32

**Telnet 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.

**SNMP ID:** 2.32.1

**Telnet 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.

**SNMP ID:** 2.32.1.1

**Telnet path:** /Setup/VLAN/Networks

## 2.32.1.2 VLAN-ID

This number uniquely identifies the VLAN.

**SNMP ID:** 2.32.1.2

**Telnet path:** /Setup/VLAN/Networks

**Possible values:**

- 0 to 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".

**SNMP ID:** 2.32.1.4

**Telnet path:** /Setup/VLAN/Networks

**Possible values:**

- Max. 251 characters

**Default:** Blank

**Note:** 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.

### 2.32.1.5 LLDP-Tx-TLV-PPID

This setting specifies to which ports, which are members of this VLAN, the device is to propagate the membership via LLDP.

**Telnet path:**

**Setup** > **VLAN** > **Networks**

**Possible values:**

Comma-separated list of interface names (analogous to the names in the column **Ports**), max. 251 characters

**Default:**

### 2.32.1.6 LLDP-Tx-TLV-Name

This setting specifies to which ports, which are members of this VLAN, the device is to propagate the name of the VLAN via LLDP.

**Telnet path:**

**Setup** > **VLAN** > **Networks**

**Possible values:**

Comma-separated list of interface names (analogous to the names in the column **Ports**), max. 251 characters

**Default:**

## 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.

**SNMP ID:** 2.32.2

**Telnet path:** /Setup/VLAN

## 2.32.2.1 Port

The name of the port; this cannot be edited.

**SNMP ID:** 2.32.2.1

**Telnet 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.

**SNMP ID:** 2.32.2.4

**Telnet path:** /Setup/VLAN/Port-Table

**Possible values:**

- Yes
- No

**Default**: Yes

## 2.32.2.5 Port-VLAN-Id

This port ID has two functions:

- Untagged packets received at this port in 'Mixed' or 'Ingress-mixed' mode are assigned to this VLAN, as are all ingress packets received in 'Never' mode.
- In the 'Mixed' 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.

**SNMP ID:** 2.32.2.5

**Telnet path:** /Setup/VLAN/Port-Table

**Possible values:**

- Max. 4 characters

**Default:** 1

### 2.32.2.6 Tagging mode

Controls the processing and assignment of VLAN tags at this port.

**SNMP ID:** 2.32.2.6

**Telnet path:** /Setup/VLAN/Port-Table

**Possible values:**

- **Never**: 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.
- **Always:** 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.
- **Mixed:** 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.
- **Ingress mixed:** Arriving (ingress) packets may or may not have a VLAN tag; outbound (egress) packets are never given a VLAN tag.

**Default:** Ingress mixed

## Tx-LLDP-TLV-Port-VLAN

Enables or disables the port as the LLDP-TLV port in this VLAN.

**WEBconfig path:** HiLCOS 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.

**SNMP ID:** 2.32.4

**Telnet path:** /Setup/VLAN

**Possible values:**

- Yes
- No

**Default:** No

**Note:** Faulty VLAN settings may cause access to the device's configuration to be blocked.

### 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'.

**SNMP ID:** 2.32.5

**Telnet path:** /Setup/VLAN

**Possible values:**

- Max. 4 characters

**Default:** 8100

## 2.34 Printer

This menu contains settings for the printer.

**SNMP ID:** 2.34

**Telnet path:** /Setup

### 2.34.1 Printer

You can adjust setting for the network printer here.

**SNMP ID:** 2.34.1

**Telnet path:** /Setup/Printer

#### 2.34.1.1 Printer

Printer name.

**SNMP ID:** 2.34.1.1

**Telnet path:** /Setup/Printer/Printer

**Possible values:**

- Max. 10 characters

**Default:** *

#### 2.34.1.2 RawIp-Port

This port can be used to accept print jobs over RawIP.

**SNMP ID:** 2.34.1.2

**Telnet path:** /Setup/Printer/Printer

**Possible values:**

- Max. 10 characters

**Default:** 9100

#### 2.34.1.3 LPD-Port

This port can be used to accept print jobs over LDP.

**SNMP ID:** 2.34.1.3

**Telnet path:** /Setup/Printer/Printer

**Possible values:**

- Max. 10 characters

**Default:** 515

## 2.34.1.4 Operating

Activates or deactivates this entry.

**SNMP ID:** 2.34.1.4

**Telnet path:** /Setup/Printer/Printer

**Possible values:**

- Yes: The print server is active.
- No: The print server is not active.

**Default:** No

## 2.34.1.5 Bidirectional

This parameter enables or disables the bi-directional mode of the printer.

**SNMP ID:** 2.34.1.5

**Telnet path:** /Setup/Printer/Printer

**Note:** 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.

## 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.

**SNMP ID:** 2.34.1.6

**Telnet path:** /Setup/Printer/Printer

**Possible values:**

- Yes
- No

**Default:** No

**Note:** Activate this option if the connection to the printer does not work as expected.

### 2.34.2 Access-List

Here you define the networks that have access to the printer.

**SNMP ID:** 2.34.2

**Telnet path:** /Setup/Printer

#### 2.34.2.1 IP-Address

IP address of the network with clients requiring access to the printer.

**SNMP ID:** 2.34.2.1

**Telnet path:** Setup/Printer/Access-list

**Possible values:**

- Valid IP address

**Default:** 0.0.0.0

#### 2.34.2.2 IP-Netmask

Netmask of the permitted networks.

**SNMP ID:** 2.34.2.2

**Telnet path:** Setup/Printer/Access-list

**Possible values:**

- Valid IP address

**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. If the routing tag is 0, access attempts from suitable IP addresses are accepted every time.

**SNMP ID:** 2.34.2.3

**Telnet path:** Setup/Printer/Access-list/Rtg-Tag

**Possible values:**

- Max. 5 characters

**Default:** Blank

**Note:** It follows that the use of routing tags only makes sense in combination with the appropriate accompanying rules in the firewall or tagged networks.

## 2.35 ECHO-Server

This menu contains the configuration of the ECHO server.

**SNMP ID:** 2.35

**Telnet path:** /Setup

### 2.35.1 Operating

The echo server is used to monitor the line quality by measuring RTT and jitter.

**SNMP ID:** 2.35.1

**Telnet path:** /Setup/ECHO-Server

**Possible values:**

- Yes

- No

**Default:** No

### 2.35.2 Access table

This table defines the access rights for using the ECHO server.

**SNMP ID:** 2.35.2

**Telnet path:** /Setup/ECHO-Server

## 2.35.2.1 IP-Address

IP address of remote device.

**SNMP ID:** 2.35.2.1

**Telnet path:** /Setup/ECHO-server/Access-table

**Possible values:**

- Valid IP address

## 2.35.2.2 Netmask

IP address of remote device.

**SNMP ID:** 2.35.2.2

**Telnet path:** /Setup/ECHO-server/Access-table

**Possible values:**

- Valid IP address

## 2.35.2.3 Protocol

Protocol used for measuring.

**SNMP ID:** 2.35.2.3

**Telnet path:** /Setup/ECHO-server/Access-table

**Possible values:**

- None
- TCP
- UDP
- TCP+UDP

### 2.35.2.4 Operating

Activates or deactivates this entry in the table.

**SNMP ID:** 2.35.2.4

**Telnet path:** /Setup/ECHO-server/Access-table

**Possible values:**

- Yes
- No

**Default:** No

### 2.35.2.5 Comment

Comment on this entry.

**SNMP ID:** 2.35.2.5

**Telnet path:** /Setup/ECHO-server/Access-table

## 2.35.3 TCP-Timeout

If a TCP session to an ECHO server is inactive for 10 (default) seconds, the server disconnects. Normally TCP clears up "dormant" connections by itself, but this takes far longer.

**SNMP ID:** 2.35.3

**Telnet path:** /Setup/ECHO-Server

**Possible values:**

- Max. 10 characters

**Default:** 10

# 2.36 Performance-Monitoring

This menu contains the configuration of the performance monitoring.

**SNMP ID:** 2.36

**Telnet path:** /Setup

## 2.36.2 RttMonAdmin

This table displays information about the type of measurements.

**SNMP ID:** 2.36.2

**Telnet path:** /Setup/Performance-Monitoring

## 2.36.2.1 Index

Shared index for the measurement

**SNMP ID:** 2.36.2.1

**Telnet path:** /Setup/Performance-Monitoring/RttMonAdmin

## 2.36.2.4 Type

Measurement type.

**SNMP ID:** 2.36.2.4

**Telnet path:** /Setup/Performance-Monitoring/RttMonAdmin

## 2.36.2.6 Frequency

Time in milliseconds until the measurement is repeated. Is the only parameter that can be modified while the status is active. In this case only 0 is allowed in order to prevent further iterations.

**SNMP ID:** 2.36.2.6

**Telnet path:** /Setup/Performance-Monitoring/RttMonAdmin

## 2.36.2.7 Timeout

Measurement timeout in milliseconds. The timeout value must be smaller than the time until measurement is repeated.

**SNMP ID:** 2.36.2.7

**Telnet path:** /Setup/Performance-Monitoring/RttMonAdmin

## 2.36.2.9 Status

Measurement status

**SNMP ID:** 2.36.2.9

**Telnet path:** /Setup/Performance-Monitoring/RttMonAdmin

**Possible values:**

- Active: Measurement is in progress. This value can only be set if the Status value is Not_In_Service. No measurement parameters can be modified while the Status is active.
- Not_In_Service: All parameters required have been set; no measurement is currently in progress.
- Not_Ready: Not all parameters required have been set.
- Create: Create a table row. SNMP Set is used to create a table row by setting the desired index to Create. When configuration is performed from the menu system the Status must also first be set to Create. When a new table row is created, the appropriate rows in the other tables are created automatically.
- Destroy: Delete a table row. This is only possible when the status is not Active. The appropriate rows in the other tables are deleted automatically.

## 2.36.3 RttMonEchoAdmin

This table displays information about the the measurements.

**SNMP ID:** 2.36.3

**Telnet path:** /Setup/Performance-Monitoring

### 2.36.3.1 Protocol

Protocol to be used

**SNMP ID:** 2.36.3.1

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.2 Destination address

Address of the responder

**SNMP ID:** 2.36.3.2

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

**Possible values:**

- Valid IP address

### 2.36.3.3 Packet size

Length of the measurement packets in bytes. Packets are padded out to the minimum length required by the measurement.

**SNMP ID:** 2.36.3.3

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.5 Destination port

Destination port. Currently ignored

**SNMP ID:** 2.36.3.5

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.17 Interval

Time between two measurement packets in milliseconds

**SNMP ID:** 2.36.3.17

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.18 Packet count

Number of measurement packets per measurement

**SNMP ID:** 2.36.3.18

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

### 2.36.3.255 Index

Shared index for the measurement

**SNMP ID:** 2.36.3.255

**Telnet path:** /Setup/Performance-Monitoring/RttMonEchoAdmin

## 2.36.4 RttMonStatistics

This table displays performance monitoring statistics.

**SNMP ID:** 2.36.4

**Telnet path:** /Setup/Performance-Monitoring

### 2.36.4.2 Completions

Number of measurements performed.

**SNMP ID:** 2.36.4.2

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.4 RTT-Count

Total number of RTT values determined

**SNMP ID:** 2.36.4.4

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.5 RTT-Sum

Sum of all RTT values determined

**SNMP ID:** 2.36.4.5

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.8 RTT-Min

Minimum roundtrip time in uSec

**SNMP ID:** 2.36.4.8

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.9 RTT-Max

Maximum roundtrip time in uSec

**SNMP ID:** 2.36.4.9

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.10 Jitter-Min-Pos-SD

Minimum positive jitter value from sender to responder in uSec

**SNMP ID:** 2.36.4.10

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.11 Jitter-Max-Pos-SD

Maximum positive jitter value from sender to responder in uSec

**SNMP ID:** 2.36.4.11

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.12 Jitter-Count-Pos-SD

Number of positive jitter values determined from sender to responder

**SNMP ID:** 2.36.4.12

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.13 Jitter-Sum-Pos-SD

Sum of all positive jitter values from sender to responder in uSec

**SNMP ID:** 2.36.4.13

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.16 Jitter-Min-Pos-DS

Minimum positive jitter value from responder to sender in uSec

**SNMP ID:** 2.36.4.16

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.17 Jitter-Max-Pos-DS

Maximum positive jitter value from responder to sender in uSec

**SNMP ID:** 2.36.4.17

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.18 Jitter-Count-Pos-DS

Number of positive jitter values determined from responder to sender

**SNMP ID:** 2.36.4.18

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.19 Jitter-Sum-Pos-DS

Sum of all positive jitter values from responder to sender in uSec

**SNMP ID:** 2.36.4.19

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.22 Jitter-Min-Neg-SD

Minimum negative jitter value from sender to responder in uSec, absolute value

**SNMP ID:** 2.36.4.22

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.23 Jitter-Max-Neg-SD

Maximum negative jitter value from sender to responder in uSec, absolute value

**SNMP ID:** 2.36.4.23

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.24 Jitter-Count-Neg-SD

Number of negative jitter values determined from sender to responder

**SNMP ID:** 2.36.4.24

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.25 Jitter-Sum-Neg-SD

Sum of all negative jitter values from sender to responder in uSec, absolute value

**SNMP ID:** 2.36.4.25

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.28 Jitter-Min-Neg-DS

Minimum negative jitter value from responder to sender in uSec, absolute value

**SNMP ID:** 2.36.4.28

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.29 Jitter-Max-Neg-DS

Maximum negative jitter value from responder to sender in uSec, absolute value

**SNMP ID:** 2.36.4.29

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.30 Jitter-Count-Neg-DS

Number of negative jitter values determined from responder to sender

**SNMP ID:** 2.36.4.30

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.31 Jitter-Sum-Neg-DS

Sum of all negative jitter values from responder to sender in uSec, absolute value

**SNMP ID:** 2.36.4.31

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.34 Packet-Loss-SD

Number of packets lost from sender to responder

**SNMP ID:** 2.36.4.34

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.35 Packet-Loss-DS

Number of packets lost from responder to sender

**SNMP ID:** 2.36.4.35

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.62 Average-Jitter

Average of all absolute jitter values

**SNMP ID:** 2.36.4.62

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.63 Average-Jitter-SD

Average of all absolute jitter values from sender to responder

**SNMP ID:** 2.36.4.63

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.64 Average-Jitter-DS

Average of all absolute jitter values from responder to sender

**SNMP ID:** 2.36.4.64

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

### 2.36.4.255 Index

Shared index for the measurement

**SNMP ID:** 2.36.4.255

**Telnet path:** /Setup/Performance-Monitoring/RttMonStatistics

# 2.37 WLAN-Management

This menu is used to configure WLAN management for WLCs.

## 2.37.1 AP-Configuration

This menu contains the settings for the AP.

**SNMP ID:** 2.37.1

**Telnet path:** /Setup/WLAN-Management

**Default:** Blank

## 2.37.1.1 Network profiles

Here you define the logical WLAN networks that can be activated and operated on the associated APs.

**SNMP ID:** 2.37.1.1

**Telnet 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.

**SNMP ID:** 2.37.1.1.1

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 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 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 logical WLAN networks to "inherit" properties from other entries.

**SNMP ID:** 2.37.1.1.2

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 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.

**SNMP ID:** 2.37.1.1.3

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of logical WLAN networks (GUI).

**Default:** All values are taken over from parent elements.

### 2.37.1.1.4 Operating

Switches the logical WLAN on or off separately.

**SNMP ID:** 2.37.1.1.4

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- On
- Off

**Default:** On

### 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.

**SNMP ID:** 2.37.1.1.6

**Telnet 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

**Default:** 802.11i-WPA-PSK (0)

**Note:** Please consider that not all wireless cards support all encryption methods.

### 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.

**SNMP ID:** 2.37.1.1.7

**Telnet 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.

**SNMP ID:** 2.37.1.1.8

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- WPA1/2
- WPA1
- WPA2

**Default:** WPA1/2 (0)

#### 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

**SNMP ID:** 2.37.1.1.9

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- ASCII character string or hexadecimal number

**Default:** Blank

#### 2.37.1.1.10 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.

**SNMP ID:** 2.37.1.1.10

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- 2.4GHz/5GHz
- 2.4GHz
- 5GHz

**Default:** 2.4GHz/5GHz

### 2.37.1.1.11 Continuation-Time

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.

**SNMP ID:** 2.37.1.1.11

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- 0 to 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.

**Note:** All other WLAN network parameters correspond to those for the standard configuration of APs.

**Note:** 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.

**Note:** 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!

### 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.

**SNMP ID:** 2.37.1.1.12

**Telnet 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.

**SNMP ID:** 2.37.1.1.13

**Telnet 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 are able to connect "faster".

**SNMP ID:** 2.37.1.1.14

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- 1M
- 2M
- 5.5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

**Default:** 2M

### 2.37.1.1.15 11b-Preambel

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.

**SNMP ID:** 2.37.1.1.15

**Telnet 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.

**SNMP ID:** 2.37.1.1.16

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Yes
- No

**Default:** No

**Note:** 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.

### 2.37.1.1.17 Cl.-Brg.-Support

Whereas address adjustment allows only the MAC address of a directly connected device to be visible to the AP, client-bridge support provides transparency; 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.

**SNMP ID:** 2.37.1.1.17

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**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

### 2.37.1.1.18 Maximum-Stations

Here you set the maximum number of clients that may associate with this AP. Additional clients wanting to associate will be rejected.

**SNMP ID:** 2.37.1.1.18

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- 0 to 65535

**Default:** 0

### 2.37.1.1.19 SSID broadcast

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.

The option **SSID broadcast** provides the following settings:

- **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).
- **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.
- **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.

**Note:** 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.

**Note:** 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.

### Telnet path:

**Telnet path:Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

### Possible values:

No

Yes

Tightened

### 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.

**SNMP ID:** 2.37.1.1.21

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Max. 32 characters

**Default:** BLANK

### 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.

**SNMP ID:** 2.37.1.1.22

**Telnet 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

**Note:** 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.

### 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.

**SNMP ID:** 2.37.1.1.23

**Telnet 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

**Note:** 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.

### 2.37.1.1.24 Short-Guard-Interval

This option is used to reduce the transmission pause between two signals from 0.8 µs (default) to 0.4 µs (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.

**SNMP ID:** 2.37.1.1.24

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Auto
- No

**Default:** Auto

### 2.37.1.1.25 Max.-Spatial-Steams

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.

**SNMP ID:** 2.37.1.1.25

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Auto
- One
- Two

**Default:** Auto

**Special values:**

- **Auto:** With the 'Auto' setting all spatial streams that are supported by the wireless LAN module in question are used.

### 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.

**SNMP ID:** 2.37.1.1.26

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.37.1.1.27 WPA2-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.

**SNMP ID:** 2.37.1.1.27

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- TKIP/AES
- AES
- TKIP

**Default:** TKIP/AES

### 2.37.1.1.28 RADIUS accounting activated

Enables or disables the RADIUS accounting on this logical WLAN network.

**Note:** The APs supporting the logical WLAN network as configured by the WLC must have a HiLCOS firmware version 8.00 or higher.

**Telnet 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).

**SNMP ID:** 2.37.1.1.30

**Telnet 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*.
- untagged: The AP forwards the packets of this SSID without any VLAN ID.

**Default:** untagged

**Note:** 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.

### 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).

**SNMP ID:** 2.37.1.1.32

**Telnet 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 to WLC-Tunnel-x (depending on 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.

**Default:** LAN

**Note:** 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.

**Note:** 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.

### 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.

**SNMP ID:** 2.37.1.1.33

**Telnet 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.

**SNMP ID:** 2.37.1.1.34

**Telnet path:** Setup/WLAN-Management/AP-Configuration/Networkprofiles

**Possible values:**

- 2 to 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 Min-Client-Strength

This entry determines the threshold, in percentage, for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the AP stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the AP and cannot associate with it. This ensures that the client has an optimized list of available APs, since the list does not contain any APs that would offer a weak connection at the client's current position.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

max. 3 characters from 0 to 9

**Default:**

0

### 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.

**Note:** APs in your network that do not support LDPC ignore this setting.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

0 to 255

**Default:**

0

### 2.37.1.1.39 IEEE802.11u-Network-Profile

Using this parameter you specify the name of an 802.11u network profile, which is to be assigned to the logical wireless network.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Profiles**, max. 32 characters

**Default:**

### 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.37.1.1.41 WPA2 key management

You configure the WPA2 key management with these options.

**Important:** 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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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*

### 2.37.1.1.48 Cl.-Brg.-Roaming-Support

Here you enable or disable the Client Bridge Roaming Support for the APs managed by the WLC.

The Client Bridge Roaming Support improves the reliability and latency of the roaming process. It is useful in situations with many devices attached to the

LAN of the Client and even more so, if most of the data traffic flows downstream; meaning, the traffic flows from the APs, through the Client to the attached devices. Enabling this feature on APs directly allows the APs to exchange information about the devices attached to a roaming Client. Enabling this feature on the Client allows freeing up the wireless link after roaming, which decreases roaming times. If this feature is enabled on the Client it will check on each roaming event if this improvement is possible or otherwise fall back on the default behavior.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

**Possible values:**

**No**

Client Bridge Roaming Support disabled

**Yes**

Client Bridge Roaming Support enabled

**Default:**

No

## 2.37.1.2 Radio profiles

Here you define the physical WLAN parameters which apply to all of the logical WLAN networks that share a managed AP.

**SNMP ID:** 2.37.1.2

**Telnet path:** /Setup/WLAN-Management/AP-Configuration

### 2.37.1.2.1 Name

Unique name for this combination of physical WLAN parameters.

**SNMP ID:** 2.37.1.2.1

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

#### 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 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.

**SNMP ID:** 2.37.1.2.2

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

#### 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.

**SNMP ID:** 2.37.1.2.3

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of logical WLAN networks (GUI).

**Default:** All values are taken over from parent elements.

#### 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.

**SNMP ID:** 2.37.1.2.4

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Albania
- Argentina
- Australia
- Austria
- Bahrain
- Bangladesh
- Belarus
- Belgium
- 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
- Kuwait
- 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

**Special values:** Default: Makes use of the encryption method defined in the 'Options' area.

### 2.37.1.2.5 Channel list

As standard the APs can use all of the channels permitted in the country of operation. To restrict the selection to certain channels, these can be entered here as a comma-separated list. Ranges can also be defined (e.g. '7–9').

**SNMP ID:** 2.37.1.2.5

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Comma-separated list with max. 48 characters

**Default:** Blank

### 2.37.1.2.6 2.4-GHz 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.

**Important:** 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.

**Telnet 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)

**Auto**
Automatic. In the 2.4-GHz mode, automatic selection provides either **11bgn-mixed** or **11bg-mixed**.

**Default:**
Auto

### 2.37.1.2.7 5-GHz 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.

**Important:** 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.

**Telnet path:**
**Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

**Possible values:**

**Normal**
802.11 g (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

**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.

**SNMP ID:** 2.37.1.2.8

**Telnet 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 (0)

### 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.

**SNMP ID:** 2.37.1.2.9

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Yes
- No

**Default:** No

**Note:** 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.

### 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.

**SNMP ID:** 2.37.1.2.10

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.37.1.2.11

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- 0 to 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.
.

**SNMP ID:** 2.37.1.2.12

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Minus 128 to 127

**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.

**SNMP ID:** 2.37.1.2.13

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- 0 to 255

**Default:** 0

**Note:** 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.

### 2.37.1.2.16 Indoor-Only-Operation

You can specify whether indoor-operation only is to be allowed.

**SNMP ID:** 2.37.1.2.16

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/WLAN-Module-2-Default/Indoor-Only-Operation

**Possible values:**

- Yes
- No

**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.

**SNMP ID:** 2.37.1.2.17

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- Yes
- No

**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.

**SNMP ID:** 2.37.1.2.18

**Telnet 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.

**SNMP ID:** 2.37.1.2.19

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Radioprofiles

**Possible values:**

- 2 to 4094

**Default:** 2

### 2.37.1.2.20 Report-seen-clients

This entry determines whether the AP should report clients detected in the WLAN network.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.37.1.2.21 Client-Steering

This entry determines whether the AP should enable band steering.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

**Possible values:**

Yes

No

**Default:**

No

### 2.37.1.2.22 Preferred-Band

This entry determines the frequency band that the AP preferably should direct the WLAN client.

**Telnet 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.

**Note:**

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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

**Possible values:**

max. 10 characters from 0 to 9

**Special values:**

0: The AP immediately considers seen probe requests as invalid.

**Default:**

120

## 2.37.1.3 Common profiles

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.

**SNMP ID:** 2.37.1.3

**Telnet path:** /Setup/WLAN-Management/AP-Configuration

### 2.37.1.3.1 Name

Name of the profile under which the settings are saved.

**SNMP ID:** 2.37.1.3.1

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Commonprofiles

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 2.37.1.3.2 Networks

List of the logical WLAN networks that are assigned via this profile.

**SNMP ID:** 2.37.1.3.2

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Commonprofiles

**Possible values:**

- Max. 251 ASCII characters, multiple values separated by commas.

**Default:** Blank

**Note:** 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.

### 2.37.1.3.3 AP parameters

A set of physical parameters that the AP WLAN modules are supposed to work with.

**SNMP ID:** 2.37.1.3.3

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Commonprofiles

**Possible values:**

- Select from the list of physical WLAN parameters (GUI) or max. 31 ASCII characters

**Default:** Blank

### 2.37.1.3.4 Controller

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).

**SNMP ID:** 2.37.1.3.4

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Commonprofiles

**Possible values:**

- IP addresses, multiple values separated by commas. Maximum 159 characters, i.e. 9 to 10 entries depending on the length of the IP addresses.

**Default:** Blank

### 2.37.1.3.6 IEEE802.11u-General

Use this parameter to specify the name of the venue profile that is to apply for the WLAN profile (i.e. the local common profile).

#### Telnet path:

**Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

#### Possible values:

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**, max. 32 characters

**Default:**

### 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.

**Telnet 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 profiles

The device LED profile selected here applies to the WLAN profile.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

**Possible values:**

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

**Default:**

*empty*

#### 2.37.1.3.248 Wireless-IDS

Here you specify the Wireless-IDS profile to the corresponding WLAN profile.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

**Possible values:**

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

### 2.37.1.4 Access points

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.

**SNMP ID:** 2.37.1.4

**Telnet path:** /Setup/WLAN-Management/AP-Configuration

#### 2.37.1.4.1 MAC-Address

MAC address of the AP.

**SNMP ID:** 2.37.1.4.1

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Valid MAC address

**Default:** Blank

**Special values:** FFFFFFFFFFFF: Defines the default configuration

#### 2.37.1.4.2 Name

Name of the AP in managed mode.

**Telnet 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.

**SNMP ID:** 2.37.1.4.3

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Max. 251 ASCII characters

**Default:** Blank

### 2.37.1.4.4 Profile

This entry sets the WLAN profile that is to be used by this AP.

**SNMP ID:** 2.37.1.4.4

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Select from the list of defined WLAN profiles, max. 31 ASCII characters.

**Default:** Blank

### 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.

**SNMP ID:** 2.37.1.4.6

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- default
- DTLS
- No

**Default:** Default

**Special values:** Default: Makes use of the encryption method defined in the 'Options' area.

### 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.

**SNMP ID:** 2.37.1.4.7

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- default
- 2.4 GHz
- 5 GHz
- Off

**Default:** Default

**Special values:** Default: Makes use of the encryption method defined in the 'Options' area.

### 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.

**SNMP ID:** 2.37.1.4.8

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- default
- 2.4 GHz
- 5 GHz
- Off

**Default:** Default

**Special values:** Default: Makes use of the encryption method defined in the 'Options' area.

### 2.37.1.4.9 Module-1-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

**SNMP ID:** 2.37.1.4.9

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Comma-separated list with max. 48 characters

**Default:** Blank

**Note:** In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

### 2.37.1.4.10 Module-2-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

**SNMP ID:** 2.37.1.4.10

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Comma-separated list with max. 48 characters

**Default:** Blank

**Note:** In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

### 2.37.1.4.11 Operating

Activates or deactivates this entry.

**SNMP ID:** 2.37.1.4.11

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Yes
- No

**Default:** Yes

### 2.37.1.4.12 IP-Address

Static IP address for the AP if DHCP cannot be /should not be used.

**SNMP ID:** 2.37.1.4.12

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Valid IP address

**Default:** Blank

### 2.37.1.4.13 Netmask

Static netmask if DHCP cannot be /should not be used.

**SNMP ID:** 2.37.1.4.13

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Valid IP address

**Default:** Blank

**Note:** Cannot be configured with LANconfig

### 2.37.1.4.14 Gateway

Static IP address of the gateway if DHCP cannot be /should not be used.

**SNMP ID:** 2.37.1.4.14

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Valid IP address

**Default:** Blank

**Note:** Cannot be configured with LANconfig

### 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.

**SNMP ID:** 2.37.1.4.16

**Telnet 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

**Default:** Auto

**Special values:** Auto: The "Auto' setting means that all available antennas are used.

### 2.37.1.4.17 AP-Intranet

This references a line in the AP intranet table.

**SNMP ID:** 2.37.1.4.17

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 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".

**SNMP ID:** 2.37.1.4.18

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Yes
- No

**Default:** Yes

**Note:** Cannot be configured with LANconfig

### 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".

**SNMP ID:** 2.37.1.4.19

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible values:**

- Blank
- Disabled_due_to_error_during_update
- Disabled_by_manual_upload

**Default:** Blank

**Note:** Cannot be configured with LANconfig

### 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 O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

**SNMP ID:** 2.37.1.4.20

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints/Module-1-Ant-Gain

**Possible Telnet values:**

- 0 to 999 dBi

**Default:** Blank

**Note:** 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'.

### 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 O-18a: Antenna gain: 18dBi, cable attenuation: 4dB --> Value to be entered = 18dBi - 4dB = 14dBi.

**SNMP ID:** 2.37.1.4.21

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints/Module-2-Ant-Gain

**Possible Telnet values:**

- 0 to 999 dBi

**Default:** Blank

**Note:** 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'.

### 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.

**SNMP ID:** 2.37.1.4.22

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible Telnet values:**

- 0 to 999 dBi

**Default:** Blank

**Note:** 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'.

### 2.37.1.4.23 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.

**SNMP ID:** 2.37.1.4.23

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Accesspoints

**Possible Telnet values:**

- 0 to 999 dBi

**Default:** Blank

**Note:** 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'.

### 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.

**Note:** 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

**Important:** The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

**Telnet 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.

**Telnet 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.

**Default:**
Automatic

### 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.

**Telnet 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.

**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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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

### 2.37.1.5 WLAN-Modul-1-Default

This setting allows you to configure the frequency band in which the AP operates the 1st physical WLAN interface.

**Telnet 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 2.4Ghz band.

**5GHz**

The AP operates the physical WLAN interface in the 5Ghz 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.

**Note:** If a managed AP only has one physical WLAN interface, the AP ignores the settings for the 2nd physical WLAN interface.

**Telnet 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 2.4Ghz band.

**5GHz**

The AP operates the physical WLAN interface in the 5Ghz 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.

**SNMP ID:** 2.37.1.7

**Telnet path:** /Setup/WLAN-Management/AP-Configuration

**Possible values:**

- DTLS
- No

**Default:** DTLS (1)

## 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.

**SNMP ID:** 2.37.1.8

**Telnet path:** /Setup/WLAN-Management/AP-Configuration

**Possible values:**

- Albania
- Argentina
- Australia
- Austria
- Bahrain
- Bangladesh
- Belarus
- Belgium
- 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
- Kuwait
- 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 (276)

## 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.

**SNMP ID:** 2.37.1.9

**Telnet 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.

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 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 rexample, 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.

**Possible values:**

- Max. 31 ASCII characters

**Default:** Blank

### 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.

**Possible values:**

- Bit field as HEX number. Set bits specify the columns to be inherited. Select from the list of intranets (GUI).

**Default:** 0

### 2.37.1.9.4 Domain name

Domain name used by the access point when resolving WLC addresses.

**Possible values:**

- Max. 63 ASCII characters

**Default:** Blank

### 2.37.1.9.5 Netmask

Static netmask if DHCP cannot be /should not be used.

**Possible values:**

- Valid IP address

**Default:** Blank

### 2.37.1.9.6 Gateway

Static IP address of the gateway if DHCP cannot be /should not be used.

**Possible values:**

- Valid IP address

**Default:** Blank

#### 2.37.1.9.7 Primary-DNS-Srv

Static IP address of the first DNS server if DHCP cannot be /should not be used.

**Possible values:**

- Valid IP address

**Default:** Blank

#### 2.37.1.9.8 Secondary-DNS-Srv

Static IP address of the second DNS server if DHCP cannot be /should not be used.

**Possible values:**

- Valid IP address

**Default:** Blank

#### 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.

**Telnet 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.

**Telnet 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.

**SNMP ID:** 2.37.1.10

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Predef.-Intranets

**Note:** 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.

#### 2.37.1.10.1 Name

This is the name of the predefined AP intranet.

**Telnet path:**/Setup/WLAN-Management/AP-Configuration/WLAN-Module-2-Default/Name

**Note:** 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.

## 2.37.1.12 DSCP-for-Control-Packets

This item allows you to set the prioritization of control packets by DiffServ (Differentiated Services).

**SNMP ID:** 2.37.1.12

**Telnet 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).

**SNMP ID:** 2.37.1.13

**Telnet 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.

  **Note:** 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.

### 2.37.1.14.1 Bridge-Interface

This item allows you to select a bridge interface for the multicast settings.

**SNMP ID:** 2.37.1.14.1

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

**Possible values:**

- Select one of the defined bridge interfaces

### 2.37.1.14.2 Active

This option activates or disables the use of CAPWAP multicast packets for this bridge interface.

**SNMP ID:** 2.37.1.14.2

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

**Possible values:**

- Yes
- No

**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.

**SNMP ID:** 2.37.1.14.3

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

**Possible values:**

- Maximum 15 characters to define a valid IP address

**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.

**SNMP ID:** 2.37.1.14.4

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

**Possible values:**

- Maximum 5 numbers to define a valid port number

**Default:** 20000 to 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.

**SNMP ID:** 2.37.1.14.5

**Telnet path:** /Setup/WLAN-Management/AP-Configuration/Multicast-Networks

**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

**Default:** 0.0.0.0

**Note:** If the list of IP networks or loopback addresses contains an entry named 'DMZ' then the associated IP address will be used. Name of a loopback 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).

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

### 2.37.1.15.0 Link calibration

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

**Possible values:**

**Off**
**Capacity**
**Robustness**

#### 2.37.1.15.1 Name

Name of the AutoWDS profile which you reference from other tables.

**Note:** The entry for the AutoWDS profile “DEFAULT” cannot be deleted or renamed.

**Telnet 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.

**Note:** Different AutoWDS profiles may not refer to the same WLAN profile.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** 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.

**Telnet 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 *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

**Telnet 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* .

**Important:** 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`.

**Telnet 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.

**Telnet 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.

**Important:** 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.

#### Telnet 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

### 2.37.1.15.19 Band

Specify the frequency band used by the APs for the AutoWDS base network.

**Telnet 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.

**Telnet 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* .

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

#### 2.37.1.16.0 Link calibration

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

**Possible values:**

**Standard**
**Off**
**Capacity**
**Robustness**

### 2.37.1.16.1 AutoWDS-Topology

Name of the AutoWDS profile for which this manual P2P configuration applies.

**Telnet 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.

**Important:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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 value

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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

String, max. 32 characters

**Default:**

#### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

Yes

No

**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.

**Note:** The prerequisite for this function is that support for connections according to IEEE 802.11u is enabled.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

Yes

No

**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.

**Telnet 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.

**Note:** 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

Yes

No

**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".

**Telnet 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.

**Note:** If your AP is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

MAC address in capital letters and without separators

**Default:**

000000000000

#### *2.37.1.17.1.10 ANQP-Profile*

Use this parameter to specify a valid ANQP profile that you want to use for the 802.11u profile.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profiles**, max. 32 characters

**Default:**

#### *2.37.1.17.1.12 HS20-Profile*

Use this parameter to specify a valid Hotspot-2.0 or HS20 profile that you want to use for the 802.11u profile.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Networkprofiles**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**, max. 32 characters

**Default:**

### 2.37.1.17.2 ANQP-Profile

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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

### *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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

String, max. 32 characters

**Default:**

### *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`.

**Note:** 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!

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

**Default:**

#### *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`.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

**Default:**

#### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

**Default:**

### *2.37.1.17.2.5 NAI-Realm-List*

Enter a valid NAI realm profile in this field.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realm-List**, max. 65 characters Multiple names can be provided in a comma-separated list.

**Default:**

### *2.37.1.17.2.6 Cellular-List*

Enter a valid cellular network profile in this field.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**, max. 65 characters. Multiple names can be provided in a comma-separated list.

**Default:**

### *2.37.1.17.2.7 Network-Auth-Type-List*

Enter one or more valid authentication parameters in this field.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **ANQP-Profile**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**, max. 65 characters. Multiple names can be provided in a comma-separated list.

**Default:**

### 2.37.1.17.3 Hotspot2.0-Profile

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.

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

**Possible values:**

String, max. 32 characters

**Default:**

#### *2.37.1.17.3.2 Operator-Name*

Enter a valid profile for hotspot operators in this field.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**, max. 65 characters

**Default:**

### *2.37.1.17.3.3 Connection-Capabilities*

Enter one or more valid entries for the connection capabilities into 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".

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Connection-Capability**, max. 250 characters Multiple names can be provided in a comma-separated list.

**Default:**

### *2.37.1.17.3.4 Operating-Class*

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*.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Hotspot2.0-Profiles**

**Possible values:**

Operating class code, max. 32 characters

**Default:**

### 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**.

**Telnet 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`.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**

**Possible values:**

String, max. 32 characters

**Default:**

#### *2.37.1.17.4.2 Network-Auth-Type*

Choose the context from the list, which applies before forwarding.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Network-Authentication-Type**

**Possible values:**

URL, max. 65 characters

**Default:**

### 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**.

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

**Possible values:**

String, max. 32 characters

**Default:**

#### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

**Possible values:**

Valid MCC, max. 3 characters

**Default:**

#### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Cellular-Network-Information-List**

**Possible values:**

Valid MNC, max. 32 characters

**Default:**

### 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u**

### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**

**Possible values:**

String, max. 65 characters

**Default:**

### *2.37.1.17.6.2 Language*

Select the language in which you store information about the location.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**

**Possible values:**

String, max. 65 characters

**Default:**

### 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**.

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

**Possible values:**

String, max. 32 characters

**Default:**

#### 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`.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

**Possible values:**

String, max. 32 characters

**Default:**

#### 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

**Telnet 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`.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **NAI-Realms**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Auth-Parameter**, max. 65 characters Multiple names can be provided in a comma-separated list.

**Default:**

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**

**Possible values:**

String, max. 32 characters

**Default:**

#### *2.37.1.17.8.2 Language*

Select a language for the hotspot operator from the list.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Operator-List**

**Possible values:**

String, max. 65 characters

**Default:**

### 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 **Common-profiles**).

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

**Possible values:**

String, max. 32 characters

**Default:**

### 2.37.1.17.9.2 Link-Status

Using this entry, you specify the connectivity status of your device to the Internet.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

**Possible values:**

0 to 4294967295, in Kbit/s

**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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

**Possible values:**

0 to 4294967295, in Kbit/s

**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.

**Telnet 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.

**Telnet 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.

**Telnet 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`: Commerce
- `Residential`: Halls of residence
- `Storage`: Warehouse
- `Utility-and-Miscellaneous`: Utility and miscellaneous
- `Vehicular`: Vehicular
- `Outdoor`: Outdoor

**Default:**

Unspecified

### *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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

## Possible values:

| *Venue group* | *Code = Venue-Type-Code* |
|---|---|
| Unspecified | |
| Assembly | ▶ 0 = unspecified assembly<br>▶ 1 = stage<br>▶ 2 = stadium<br>▶ 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station)<br>▶ 4 = amphitheater<br>▶ 5 = amusement park<br>▶ 6 = place of worship<br>▶ 7 = convention center<br>▶ 8 = library<br>▶ 9 = museum<br>▶ 10 = restaurant<br>▶ 11 = theater<br>▶ 12 = bar<br>▶ 13 = café<br>▶ 14 = zoo, aquarium<br>▶ 15 = emergency control center |
| Business | ▶ 0 = unspecified business<br>▶ 1 = doctor's office<br>▶ 2 = bank<br>▶ 3 = fire station<br>▶ 4 = police station<br>▶ 6 = post office<br>▶ 7 = office<br>▶ 8 = research facility<br>▶ 9 = law firm |
| Educational: | ▶ 0 = unspecified education<br>▶ 1 = primary school<br>▶ 2 = secondary school<br>▶ 3 = college |
| Factory and industry | ▶ 0 = unspecified factory and industry<br>▶ 1 = factory |
| Institutional | ▶ 0 = unspecified institution<br>▶ 1 = hospital<br>▶ 2 = long-term care facility (e.g., nursing home, hospice)<br>▶ 3 = rehabilitation clinic<br>▶ 4 = organizational association<br>▶ 5 = prison |
| Commerce | ▶ 0 = unspecified commerce |

| *Venue group* | *Code = Venue-Type-Code* |
|---|---|
| | ▶ 1 = retail store<br>▶ 2 = food store<br>▶ 3 = Automobile workshop<br>▶ 4 = shopping center<br>▶ 5 = gas station |
| Halls of residence | ▶ 0 = unspecified residence hall<br>▶ 1 = private residence<br>▶ 2 = hotel or motel<br>▶ 3 = student housing<br>▶ 4 = guesthouse |
| Warehouse | ▶ 0 = unspecified warehouse |
| Utility and miscellaneous | ▶ 0 = unspecified service and miscellaneous |
| Vehicular | ▶ 0 = unspecified vehicle<br>▶ 1 = passenger or transport vehicles<br>▶ 2 = aircraft<br>▶ 3 = bus<br>▶ 4 = ferry<br>▶ 5 = ship or boat<br>▶ 6 = train<br>▶ 7 = motorcycle |
| Outdoor | ▶ 0 = unspecified outdoor<br>▶ 1 = Municipal WLAN network<br>▶ 2 = city park<br>▶ 3 = rest area<br>▶ 4 = traffic control<br>▶ 5 = bus stop<br>▶ 6 = kiosk |

*Table 15: Overview of possible values for venue groups and types*

**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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **General**

**Possible values:**

**Name** from the table **Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Venue-Name**, max. 32 characters. Multiple names can be provided in a hash-sign-separated ('#') list.

**Default:**

### 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**.

| *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 |

| *Parameter* | *Sub-Parameter* | *Comment* |
|---|---|---|
| | NFCSecure* | NFC chip |
| | HWToken* | Hardware token |
| | SoftToken* | Software token |
| | Certificate* | Digital certificate |
| | UserPass* | Username and password |
| | Anonymous* | Anonymous login |

*Table 16: Overview of possible authentication parameters*

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

**Telnet 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**.

**Telnet 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**).

**Telnet 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**.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **IEEE802.11u** > **Connection-Capability**

## 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.).

**Important:** An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups should overlap, HiLCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status** > **WLAN-Management** > **AP-Configuration**.

**Important:** 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

### 2.37.1.18.1 Name

Name of the assignment group which you reference from other tables.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

### 2.37.1.21.1 Name

Give a name to the device LED profile here.

**Telnet 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.

**Telnet 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.

**Telnet 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).

**Telnet 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).

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS**

#### *2.37.1.22.1.1 Name*

Enter a description of the device.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

**Possible values:**

**Yes**
**No**

**Default:**

No

#### *2.37.1.22.1.3 Use TLS connection*

This setting determines whether the connection to the LBS server is SSL/TLS secured.

**Note:** Modifying this setting requires the LBS to be restarted.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

**Possible values:**

**Yes**
**No**

#### *2.37.1.22.1.4 LBS server address*

Enter the address of the LBS server.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**

**Possible values:**

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

**Default:**

9090

### 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).

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS**

#### *2.37.1.22.2.1 Name*

Enter a description of the device.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

Max. 6 characters from `[0-9]-`

**Default:**

0

### *2.37.1.22.2.4 Latitude*

This value specifies the angle of the latitude in degrees.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 90

**Default:**

0

### *2.37.1.22.2.5 Latitude minutes*

This value specifies the minutes value of the latitude.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 60

**Default:**

0

### *2.37.1.22.2.6 Latitude seconds*

This value specifies the seconds value of the latitude.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 60

**Default:**

0

### *2.37.1.22.2.7 Latitude hemisphere*

This value specifies the orientation of the latitude. Possible values are:

- N: Northerly latitude
- S: Southerly latitude

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

**N**
**S**

**Default:**

N

### *2.37.1.22.2.8 Longitude*

This value specifies the angle of the longitude in degrees.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 90

**Default:**

0

### *2.37.1.22.2.9 Longitude minutes*

This value specifies the minutes value of the longitude.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 60

**Default:**

0

### *2.37.1.22.2.10 Longitude seconds*

This value specifies the seconds value of the longitude.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

0 … 60

**Default:**

0

### *2.37.1.22.2.8 Longitude hemisphere*

This value specifies the orientation of the longitude. Possible values are:

- W: Western longitude
- E: Eastern longitude

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

**O**
**W**

**Default:**

W

#### *2.37.1.22.2.12 Description*

Enter a description of the device.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **Device-Location**

**Possible values:**

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

**Default:**

*empty*

## 2.37.1.23 Wireless ePaper profile

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

### 2.37.1.23.1 Name

Specify the name of the Wireless ePaper profile here.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-ePaper-Profile**

**Possible values:**

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

1 … 65535 Integer value

**Default:**

7353

### 2.37.1.24 iBeacon-Profiles

**Telnet 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.

**Telnet 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

**Telnet 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.

**Telnet 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.

**Telnet 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

### 2.37.1.248 Wireless-IDS

At this point you make the settings for the Wireless IDS.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

#### 2.37.1.248.1 Name

Here you specify the name of the Wireless IDS profile.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

### 2.37.1.248.2 Operating

Activates or deactivates Wireless IDS.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

Wireless IDS deactivated

**Yes**

Wireless IDS activated

**Default:**

Yes

### 2.37.1.248.3 EAPOLStartCounterLimit

Set the threshold value for the EAPOL-Start frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.4 EAPOLStartCounterInterval

Specify the period of time in which the EAPOL-Start frames are counted here. If the device counts more EAPOL-Start frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.5 ProbeBroadCounterLimit

Set the threshold value for the broadcast probe frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

500

### 2.37.1.248.6 ProbeBroadCounterInterval

Specify the period of time in which the broadcast probe frames are counted here. If the device counts more broadcast probe frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.7 DeauthenticateBroadCounterLimit

Set the threshold value for broadcast deauthenticate frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

2

### 2.37.1.248.8 DeauthenticateBroadCounterInterval

Here you specify the period of time in which the broadcast deauthenticate frames are counted. If the device counts more broadcast deauthenticate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

1

### 2.37.1.248.9 DeauthenticateCounterLimit

Set the threshold value for deauthenticate frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.10 DeauthenticateCounterInterval

Here you specify the period of time in which the deauthenticate frames are counted. If the device counts more deauthenticate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.11 AssociateReqCounterLimit

Set the threshold value for associate request frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.12 AssociateReqCounterInterval

Here you specify the period of time in which the associate request frames are counted. If the device counts more associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.13 ReAssociateReqCounterLimit

Set the threshold value for re-associate request frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.14 ReAssociateReqCounterInterval

Here you specify the period of time in which the re-associate request frames are counted. If the device counts more re-associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.15 AuthenticateCounterLimit

Set the threshold value for authenticate request frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.16 AuthenticateCounterInterval

Here you specify the period of time in which the authenticate request frames are counted. If the device counts more authenticate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.17 DisAssociateCounterLimit

Set the threshold value for dis-associate request frames here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

250

### 2.37.1.248.18 DisAssociateCounterInterval

Here you specify the period of time in which the dis-associate request frames are counted. If the device counts more dis-associate request frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

10

### 2.37.1.248.19 IDS-Operational

Enable or disable Wireless IDS here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

Wireless IDS disabled

**Yes**

Wireless IDS enabled

**Default:**

No

### 2.37.1.248.20 SyslogOperational

Enable or disable the creation of syslog entries via Wireless IDS here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

Creation of syslog entries via Wireless IDS disabled

**Yes**

Creation of syslog entries via Wireless IDS enabled

**Default:**

Yes

### 2.37.1.248.21 SNMPTraps-Operational

Enable or disable the sending of traps via Wireless IDS.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

Sending traps via Wireless IDS disabled

**Yes**

Sending traps via Wireless IDS enabled

**Default:**

No

### 2.37.1.248.22 E-Mail

Enable or disable e-mail notifications via Wireless IDS here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

E-mail notifications via Wireless IDS disabled

**Yes**

E-mail notifications via Wireless IDS enabled

**Default:**

No

### 2.37.1.248.23 E-Mail-Receiver

Specify the e-mail destination address here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

### 2.37.1.248.24 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.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

E-mail sending for each event

**Default:**

10

### 2.37.1.248.26 BlockAckOutOfWindowCounterLimit

Here you set the threshold value on the out-of-window frames that are received during a block-ack session.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

200

### 2.37.1.248.27 BlockAckOutOfWindowCounterInterval

Here you specify the time interval for counting the out-of-window frames. If the device counts more out-of-window frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.28 BlockAckAfterDelBACounterLimit

Here you set the threshold value for block-ACK-session frames that arrive after receiving the DELBA frame.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

100

### 2.37.1.248.29 BlockAckAfterDelBACounterInterval

Here you specify the time interval for counting the Block-Ack-session frames. If the device counts more Block-Ack-session frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.31 NullDataFloodCounterLimit

Here you set the threshold value for received null-data frames.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

500

### 2.37.1.248.32 NullDataFloodCounterInterval

Here you specify the time interval for counting the null-data frames. If the device counts more null-data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.34 NullDataPSBufferOverflowCounterLimit

Here you set the threshold value for the data frames that were deleted due to a buffer overflow.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

200

### 2.37.1.248.35 NullDataPSBufferOverflowCounterInterval

Here you specify the time interval for counting the deleted data frames. If the device counts more data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.37 PSPollTIMInterval

Here you specify when, at the earliest, the client is allowed to send a PS-poll frame to the AP before the specified TIM interval expires.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

5

### 2.37.1.248.38 PSPollTIMIntervalCounterLimit

Here you set the threshold value for the PS-poll frames that are received after the listen interval difference is exceeded.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

100

### 2.37.1.248.39 PSPollTIMIntervalCounterInterval

Here you specify the time interval for counting the PS-poll frames. The program triggers an alarm if, within this time interval, the device counts any additional PS-poll frames arriving after the "PSPollTIMIntervalDiff" is exceeded and that exceed the limit set for the "PSPollTIMIntervalDiffCounter".

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.41 SMPSMulStreamCounterLimit

Here you specify the threshold value for the number of data frames the client transmits using multiple spatial streams after the client has switched into the static SM power save mode.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**

100

### 2.37.1.248.42 SMPSMulStreamCounterInterval

Here you specify the time interval for counting the data frames the client transmits using multiple spatial streams. If the device counts more data frames within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

5

### 2.37.1.248.43 SMPSSingleStreamCounterLimit

Here you specify the threshold value for the number of failed data frame transmissions from the AP using multiple spatial streams to the client after the client has disabled the static SM power save mode.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Default:**
100

### 2.37.1.248.44 SMPSSingleStreamCounterInterval

Here you specify the time interval for counting the failed data frame transmissions from the AP using multiple spatial streams. If the device counts more failed data frame transmissions within the time interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**
**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**
Max. 4 characters from `[0-9]`

**Special values:**

**0**
Switches the function off.

**Default:**
5

### 2.37.1.248.45 DisAssociateBroadCounterLimit

Set the threshold value for broadcast disassociate frames here.

**Telnet path:**
**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**
Max. 4 characters from `[0-9]`

**Default:**

2

### 2.37.1.248.46 DisAssociateBroadCounterInterval

Here you specify the period of time in which the broadcast disassociate frames are counted. If the device counts more broadcast disassociate frames within the interval than are specified in the threshold value, then the program triggers an alarm.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

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

**Special values:**

**0**

Switches the function off.

**Default:**

1

### 2.37.1.248.52 Intruder-Identification

Enable or disable Wireless IDS intruder identification here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

Wireless IDS intruder identification is disabled

**Yes**
Wireless IDS intruder identification is enabled

**Default:**
No

### 2.37.1.248.53 Timeout-Intruder-Activity

Here you specify the time following an attack after which the status of the attacker is set to inactive.

**Telnet path:**
**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**
Max. 4 characters from `[0-9]`

**Default:**
60

### 2.37.1.248.54 White-List-Id

Here you specify the White List ID for the white list of the Wireless IDS profile. This White List ID is used to group the stations that are to be excluded from the intruder identification into white lists for the corresponding Wireless IDS profile.

**Telnet path:**
**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**
Max. 4 characters from `[0-9]`

#### 2.37.1.248.55 Store-Intruder-DHCP-Requests

Enable or disable the storage of intruder DHCP requests here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Wireless-IDS**

**Possible values:**

**No**

The storage of intruder DHCP requests is disabled

**Yes**

The storage of intruder DHCP requests is enabled

**Default:**

No

### 2.37.1.249 WIDS-White-List-Table

Here you configure the entries in the white lists for the corresponding Wireless IDS profile. These entries specify the stations for exclusion from the intruder identification.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

#### 2.37.1.249.1 Index

Specify the index for the entry here.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **WIDS-White-List-Table**

**Possible values:**

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

### 2.37.1.249.2 White-List-Id

Enter the White List ID that fits to the Wireless IDS profile here. You use the White List ID to assign those stations that are to be excluded from the intruder identification to the white lists for the corresponding Wireless IDS profile.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **WIDS-White-List-Table**

**Possible values:**

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

### 2.37.1.249.3 Station-MAC

Here you specify the MAC address of the station that is to be excluded from intruder identification.

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **WIDS-White-List-Table**

**Possible values:**

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

## 2.37.5 CAPWAP-Port

Port number for the CAPWAP service

**SNMP ID:** 2.37.5

**Telnet path:** /Setup/WLAN-Management

**Possible values:**

- 0 to 65535

**Default:** 1027

**Note:** Cannot be configured with LANconfig

## 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.

**SNMP ID:** 2.37.6

**Telnet path:** /Setup/WLAN-Management

**Possible values:**

- Yes
- No

**Default:** No

**Note:** 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.

## 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 HiLCOS 9.00

```
[-c] <WTP-MAC> [<Profile>] [<Name>] [<IP>] [<Netmask>] [<Gateway>]
```

### Syntax used in versions as of HiLCOS 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>]
```

**Note:** If you define multiple MAC addresses, the device ignores the arguments `[-i <IP>]` and `[-n <Name>]`.

### Telnet 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 HiLCOS 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).

**SNMP ID:** 2.37.8

**Telnet path:** /Setup/WLAN-Management

**Possible values:**

- Yes
- No

**Default:** No

**Note:** 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.

## 2.37.9 Disconnect-AP

Do command to disconnect APs. The MAC address must be specified as a parameter.

**SNMP ID:** 2.37.9

**Telnet path:** /Setup/WLAN-Management

**Possible values:**

- Syntax: do Disconnect-AP <WTP-MAC>

**Default:** Blank

## 2.37.10 Notification

This menu contains the configuration of the notification system of the WLAN management.

**SNMP ID:** 2.37.10

**Telnet path:** /Setup/WLAN-Management

## 2.37.10.1 E-Mail

Activates notification by e-mail.

**SNMP ID:** 2.37.10.1

**Telnet path:** /Setup/WLAN-Management/Notification

**Possible values:**

- Yes
- No

**Default:** No

## 2.37.10.2 Syslog

Activates notification by SYSLOG.

**SNMP ID:** 2.37.10.2

**Telnet path:** /Setup/WLAN-Management/Notification

**Possible values:**

- Yes
- No

**Default:** No

## 2.37.10.3 E-Mail-Receiver

Information about events in the WLC is sent to this e-mail address.

**SNMP ID:** 2.37.10.3

**Telnet path:** /Setup/WLAN-Management/Notification

**Possible values:**

- Valid e-mail address with up to 63 ASCII characters

**Default:** Blank

**Note:** An SMTP account must be set up to make use of e-mail messaging.

## 2.37.10.4 Advanced

Here you define the events that you wish to be informed of.

**SNMP ID:** 2.37.10.4

**Telnet path:** /Setup/WLAN-Management/Notification

### 2.37.10.4.1 Name

Selects the events that trigger notification.

**SNMP ID:** 2.37.10.4.1

**Telnet path:** /Setup/WLAN-Management/Notification/Advanced

**Possible values:**

- E-mail
- Syslog

**Default:** Blank

**Special values:** Value is fixed

### 2.37.10.4.2 Active-Radios

Activates notification about active APs.

**SNMP ID:** 2.37.10.4.2

**Telnet path:** /Setup/WLAN-Management/Notification/Advanced

**Possible values:**

- Yes
- No

**Default:** No

### 2.37.10.4.3 Missing-AP

Activates notification about lost APs.

**SNMP ID:** 2.37.10.4.3

**Telnet path:** /Setup/WLAN-Management/Notification/Advanced

**Possible values:**

- Yes
- No

**Default:** No

#### 2.37.10.4.4 New-AP

Activates notification about new APs.

**SNMP ID:** 2.37.10.4.4

**Telnet 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.

**Telnet path:**/Setup/WLAN-Management/Notification/Send-SNMP-Trap-for-Station-Table-Event

**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.

**SNMP ID:** 2.37.19

**Telnet path:** /Setup/WLAN-Management

**Possible values:**

- Syntax: do Start-automatic-radio-field-optimization [<WTP-MAC>]

**Default:** Blank

## 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.

**Telnet path:**

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

## 2.37.21.1 MAC address pattern

Enter the MAC address of a station.

**Note:** It is possible to use wildcards.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Important:** The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

**Note:** This field has no significance for networks secured by WEP.

**Telnet 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.

**Note:** 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".

**Telnet 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.

**Note:** 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".

**Telnet 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.

**Telnet 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.

**Note:** The use of wildcards makes it possible to allow access to multiple SSIDs.

**Telnet 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.

**SNMP ID:** 2.37.27

**Telnet path:** /Setup/WLAN-Management

## 2.37.27.11 Firmware-Depot-URL

Directory where the latest firmware files are stored

**SNMP ID:** 2.37.27.11

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management

**Possible values:**

- URL in the form Server/Directory or http://Server/Directory

**Default:** Blank

## 2.37.27.12 Script-Depot-URL

The path to the directory with the script files.

**SNMP ID:** 2.37.27.12

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management

**Possible values:**

- URL in the form Server/Directory or http://Server/Directory

**Default:** Blank

## 2.37.27.13 Update-Firmware-and-Script-Information

Launches an update process for the available firmware and script information

**SNMP ID:** 2.37.27.13

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management

**Possible values:**

- Syntax: do Update-Firmware-and-Script-Information

**Note:** Do command

## 2.37.27.14 Maximum-Number-Of-Loaded-Firmwares

Maximum number of firmware versions in memory

**SNMP ID:** 2.37.27.14

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management

**Possible values:**

- 1 to 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.

**SNMP ID:** 2.37.27.15

**Telnet 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.

**SNMP ID:** 2.37.27.15.2

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

**Possible values:**

- All, or a selection from the list of available devices.

**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.

**SNMP ID:** 2.37.27.15.3

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

**Possible values:**

- Valid MAC address

**Default:** Blank

### 2.37.27.15.4 Version

Firmware version that is to be used for the devices or device types specified here.

**SNMP ID:** 2.37.27.15.4

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management/Firmware-Version-Management

**Possible values:**

- Firmware version in the form X.XX

**Default:** Blank

### 2.37.27.15.5 Date

Date of the corresponding firmware version.

### Telnet 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 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 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 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.

**SNMP ID:** 2.37.27.16

**Telnet 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.

**SNMP ID:** 2.37.27.16.1

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management/Script-Management

**Possible values:**

- Select from the list of defined WLAN profiles, maximum 31 ASCII characters.

**Default:** Blank

### 2.37.27.16.2 Name

Name of the script file to be used.

**SNMP ID:** 2.37.27.16.2

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management/Script-Management

**Possible values:**

- File name in the form *.lcs, max. 63 ASCII characters

**Default:** Blank

## 2.37.27.18 Reboot-updated-APs

Reboot updated APs.

**SNMP ID:** 2.37.27.18

**Telnet path:** /Setup/WLAN-Management/Central-Firmware-Management

**Possible values:**

- Syntax: Do Reboot-updated-APs

**Note:** Do command

## 2.37.27.25 Firmware-Loopback-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.

**SNMP ID:** 2.37.27.25

**Telnet 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.

**Default:** Blank

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

## 2.37.27.26 Script-Loopback-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.

**SNMP ID:** 2.37.27.26

**Telnet 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.

**Default:** Blank

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

## 2.37.27.38 Max. number of concurrent updates

Here you specify how many firmware updates the WLC may perform at the same time.

**Telnet path:**

**Setup** > **WLAN-Management** > **Central-Firmware-Management**

**Possible values:**

**1-30**
**10**

**Default:**

10

## 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.

**Telnet 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.

**SNMP ID:** 2.37.30

**Telnet path:** /Setup/WLAN-Management/Sync-WTP-Password

**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.

**Telnet path:**/Setup/WLAN-Management/Interval-for-status-table-cleanup

**Possible values:**

- Max. 11 numerical characters

**Default:** 1440 minutes

## 2.37.32 License count

This value indicates the current number of licenses for the WLC that you can use on this device.

**SNMP ID:** 2.37.32

**Telnet path:** /Setup/WLAN-Management/License-Count

**Note:** This value is for your information only. You cannot change it.

## 2.37.33 License limit

This value indicates the maximum possible number of licenses for the WLC that you can use on this device.

**Telnet path:**/Setup/WLAN-Management/License-limit

**Note:** This value is for your information only. You cannot change it.

## 2.37.34 WLC cluster

This menu contains the settings for the data connections and status connections between multiple WLCs (WLC cluster).

**Telnet 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.

**Important:** 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.

**Tip:** 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.

**Telnet 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.

**Note:** The WLCs can only interconnect if they have a certificate from the same certificate hierarchy.

**Telnet 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.

**Telnet 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.

**Note:** If the source address set here is a loopback address, these will be used on the remote client. **unmasked** !

**Telnet 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**

**Note:** 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.

**Telnet 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.

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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

### 2.37.35 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

**Note:** 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

**Note:** 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.

**Telnet 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.

**Telnet 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.

**Telnet 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`).

**Telnet 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**.

**Note:** Statistics capture increases the load on the WLC. Hirschmann does not recommend the permanent recording of statistics.

**Telnet 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.

**Telnet path:**
**Status** > **WLAN-Management** > **Client-Steering**

### 2.37.40.19.1 Name

Name of the client-steering profile.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Note:** The recording of statistical data is enabled elsewhere using the parameter *2.37.40.17 Acquire-statistical-data* on page 1176.

**Telnet path:**

**Status** > **WLAN-Management** > **Band-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.

**Note:** To find out whether a specific device supports LLDP, refer to the corresponding data sheet.

**Telnet path:**

**Setup** > **LLDP**

## 2.38.1 Message-TX-Interval

This value defines the interval in seconds for the regular transmission of LLDPDUs by the device.

**Note:** If the device detects changes to the LLDP information during an interval, the device can send additional LLDP messages. The *Tx delay* parameter defines the maximum frequency of LLDP messages caused by these changes.

**Note:** 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*,

**Telnet path:**

**Setup** > **LLDP** > **Message-TX-interval**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **LLDP** > **Message-TX-Hold-Multiplier**

**Possible values:**

0 to 99

**Default:**

4

### 2.38.3 Reinit-Delay

This value defines the time the device suppresses transmission of LLDPDUs even though the LLDP is activated.

**Telnet path:**

**Setup** > **LLDP** > **Reinit-Delay**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **LLDP** > **Tx-Delay**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **LLDP** > **Notification-Interval**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **LLDP** > **Ports**

## 2.38.6.1 Name

The name of the port or interface

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **Name**

**Possible values:**

Depending on the interfaces, e.g., LAN-1, WLAN-1

### 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.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **Admin-Status**

**Possible values:**

Off

Tx-Only

Rx-Only

Rx/Tx

**Default:**

Off

### 2.38.6.3 Notification

Use this to set whether changes in an MSAP remote station for this port are reported to possible network management systems.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **Notifications**

**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.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **TLVs**

**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.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **TLVs-802.3**

**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.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **Max-Neighbors**

**Possible values:**

0 to 65535

**Default:**

0

### 2.38.6.8 Update-Source

This parameter specifies the optional sources for LLDP updates.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **Update-Source**

**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.

**Telnet path:**

**Setup** > **LLDP** > **Ports** > **TLVs-LCS**

**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.

**Telnet path:**

**Setup** > **LLDP** > **Management-Addresses**

**Note:** 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.

### 2.38.7.1 Network-Name

The name of the TCP/IP network, as entered in the TCP-IP network list.

**Telnet path:**

**Setup** > **LLDP** > **Management-Addressen** > **Network-Name**

**Possible values:**

Max. 16 alphanumerical characters

**Default:**

Blank

### 2.38.7.2 Port-List

The list of interfaces and ports belonging to the corresponding management address.

**Telnet path:**

**Setup** > **LLDP** > **Management-Addresses** > **Port-List**

**Possible values:**

>Comma-separated list of ports, max 251 alphanumeric characters, e.g., LAN-1 or WLAN-1. Use wildcards to specify a group of ports (e.g., "*_*" ).

**Default:**

Blank

## 2.38.8 Protocol

This table contains the LLDP port settings for the spanning-tree and rapid-spanning-tree protocols.

**Telnet path:**

**Setup** > **LLDP** > **Protocols**

### 2.38.8.1 Protocol

This parameter sets the protocol for which the LLDP ports are enabled.

**Telnet path:**

**Setup** > **LLDP** > **Protocols** > **Protocol**

**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).

**Telnet path:**

**Setup** > **LLDP** > **Protocols** > **Port-List**

**Possible values:**

>Comma-separated list of ports, max 251 alphanumeric characters, e.g., LAN-1 or WLAN-1. Use wildcards to specify a group of ports (e.g., "*_*" ).

**Default:**

Blank

### 2.38.9 Immediate-Delete

This parameter enables or disables the direct deletion of LLDPDUs.

**Telnet path:**

**Setup** > **LLDP** > **Immediate-Deletion**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.38.10 Operating

This parameter enables or disables the use of LLDP.

**Telnet path:**

**Setup** > **LLDP** > **Operating**

**Possible values:**

Yes

No

**Default:**

Yes

# 2.39 Certificates

This menu contains the configuration of the certificates.

**SNMP ID:** 2.39

**Telnet path:** /Setup

## 2.39.1 SCEP-Client

This menu contains the configuration of the SCEP client.

**SNMP ID:** 2.39.1

**Telnet path:** /Setup/Certificates

### 2.39.1.1 Operating

Turns the usage of SCEP on or off.

**SNMP ID:** 2.39.1.1

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- Yes
- No

**Default:** No

**Special values:** No

### 2.39.1.2 Device-Certificate-Update-Before

Preparation time in days for the timely retrieval of new RA/CA certificates.

**SNMP ID:** 2.39.1.2

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- Max. 10 characters

**Default:** Blank

### 2.39.1.3 Device-Certificate-Update-Before

Preparation time in days for the timely retrieval of new RA/CA certificates.

**SNMP ID:** 2.39.1.3

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- Max. 10 characters

**Default:** 3

### 2.39.1.7 Certificates

Here you can configure certificates or add new ones.

**SNMP ID:** 2.39.1.7

**Telnet path:** /Setup/Certificates/SCEP-Client

#### 2.39.1.7.1 Name

The certificate's configuration name.

**SNMP ID:** 2.39.1.7.1

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 16 characters

**Default:** Blank

### 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 HiLCOS variables:

- %% 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 serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

**SNMP ID:** 2.39.1.7.2

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 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 HiLCOS variables:

- %% 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 serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

**SNMP ID:** 2.39.1.7.3

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 2.39.1.7.4 ChallengePwd

Password (for the automatic issue of device certificates on the SCEP server).

**SNMP ID:** 2.39.1.7.4

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

#### 2.39.1.7.5 SubjectAltName

Further information about the requester, e.g. domain or IP address.

**SNMP ID:** 2.39.1.7.5

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

#### 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)

**SNMP ID:** 2.39.1.7.6

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

#### 2.39.1.7.7 Device-Certificate-Keylength

The length of the key to be generated for the device itself.

**SNMP ID:** 2.39.1.7.7

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- 31 or better

**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.

**SNMP ID:** 2.39.1.7.8

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- VPN

**Default:** VPN

#### 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

**SNMP ID:** 2.39.1.7.9

**Telnet path:** /Setup/Certificates/SCEP-client/Certificates

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.39.1.10

**Telnet path:** /Setup/Certificates/SCEP-Client

## 2.39.1.11 Retry-After-Error-Interval

Interval in seconds between retries after errors of any type.

**SNMP ID:** 2.39.1.11

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- Max. 10 characters

**Default:** 22

## 2.39.1.12 Check-Pending-Requests-Interval

Interval in seconds for checks on outstanding certificate requests.

**SNMP ID:** 2.39.1.12

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.39.1.13

**Telnet path:** /Setup/Certificates/SCEP-Client

**Possible values:**

- All: All trace messages, including information and debug messages
- Reduced: Error and alert messages only
- Only errors: Error messages only

**Default:**

All

## 2.39.1.14 CAs

This table is used to define the available CAs.

**SNMP ID:** 2.39.1.14

**Telnet path:** /Setup/Certificates/SCEP-Client/CAs

#### 2.39.1.14.1 Name

Enter a name that identifies this configuration.

**SNMP ID:** 2.39.1.14.1

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/Name

**Possible values:** Max. 16 alphanumerical characters

**Default:** Blank

#### 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

**SNMP ID:** 2.39.1.14.2

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/URL

**Possible values:**

- Max. 251 alphanumerical characters

**Default:** Blank

#### 2.39.1.14.3 DN

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=HIRSCHMANN CA/O=HIRSCHMANN/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 HiLCOS variables:

- %% 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 serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

**SNMP ID:** 2.39.1.14.3

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/DN

**Possible values:**

- Max. 251 alphanumerical characters

**Default:** Blank

### 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:

**Note:** 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.

**Telnet 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.

**Default:**

DES

### 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.

**SNMP ID:** 2.39.1.14.5

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/Identifier

**Possible values:**

- Max. 251 alphanumerical characters

**Default:** Blank

### 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.

**Telnet 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.

**SNMP ID:** 2.39.1.14.7

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/RA-Autoapprove

**Possible values:**

- Yes
- No

**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.

**Telnet 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: ' :' ' -' ' ,' ' '

**SNMP ID:** 2.39.1.14.9

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/CA-Fingerprint

**Possible values:**

- Max. 59 alphanumerical characters

**Default:** Blank

### 2.39.1.14.11 Loopback-Addr.

Enter a loopback address.

**SNMP ID:** 2.39.1.14.11

**Telnet path:** /Setup/Certificates/SCEP-Client/Certificates/Loopback-Addr.

**Possible values:** Max. 16 characters

**Default:** Blank

### 2.39.2 SCEP-CA

This menu contains the settings for SCEP-CA.

**SNMP ID:** 2.39.2

**Telnet path:** /Setup/Certificates/SCEP-Client

## 2.39.2.1 Operating

Activates or deactivates the SCEP client.

**SNMP ID:** 2.39.2.1

**Telnet path:** /Setup/Certificates/SCEP-CA/SCEP-Operating

**Possible values:**

- Yes
- No

**Default:** No

## 2.39.2.2 CA-certificates

This menu contains the settings for CA certificates.

**SNMP ID:** 2.39.2.2

**Telnet path:** /Setup/Certificates/SCEP-Client/CAs

#### 2.39.2.2.1 CA-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=HIRSCHMANN CA/O=HIRSCHMANN/C=DE

**SNMP ID:** 2.39.2.2.1

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-Certificates/CA-Distinguished-Name

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 2.39.2.2.3 Alternative-Name

An alternative 'Subject Name' can be entered here.

**Examples:** Critical, DNS:host.company.de IP:10.10.10.10 DNS:host.company.de, IP:10.10.10.10 UFQDN:email:name@company.de

**SNMP ID:** 2.39.2.2.3

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-Certificates/Alternative-Name

### 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.

**SNMP ID:** 2.39.2.2.4

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-Certificates/RSA-Key-Length

**Possible values:**

- 1024
- 2048
- 3072
- 4096
- 8192

**Default:** 2048

**Note:** The time taken for calculation depends on the performance available from the system; the greater the number of bits, the longer it takes.

### 2.39.2.2.5 Validity period

Here you enter the certificate's validity period in days.

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Validity-Period

**Possible values:**

- Max. 5 numerical characters

**Default:** 1100

### 2.39.1.2 Update-CA-certificates-before-expiration

Enter the time period for the 'Update before expiry' in days.

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Update-CA-certificates-before-expiration

**Possible values:**

- Max. 2 numerical characters

**Default:** 4

### 2.39.2.2.8 RA-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=HIRSCHMANN CA/O=HIRSCHMANN/C=DE

**SNMP ID:** 2.39.2.2.8

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-Certificates/RA-Distinguished-Name

**Possible values:**

- Max. 251 characters

**Default:** Blank

### 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.

**SNMP ID:** 2.39.2.2.9

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Create-new-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.

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Create-PKCS12-Backup-Files

### 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.

**SNMP ID:** 2.39.2.2.11

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Restore-certificates-from-Backup

## 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:

**Note:** 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.

### Telnet 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.

**Telnet path:** /Setup/Certificates/SCEP-CA/RA-Autoapprove

**Possible values:**

- Yes
- No

**Default:** Yes

## 2.39.2.5 Client-Certificates

This menu contains the settings for client certificates.

**SNMP ID:** 2.39.2.5

**Telnet path:** /Setup/Certificates/SCEP-CA/Client-Certificates

### 2.39.2.5.1 Validity period

Here you specify the validity period of the certificate in days.

**Telnet path:** /Setup/Certificates/SCEP-CA/CA-certificates/Validity-Period

**Possible values:**

- Max. 5 numerical characters

**Default:** 365

### 2.39.2.5.3 Challenge passwords

This table provides an overview of the challenge passwords.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **Client-Certificates**

#### *2.39.2.5.3.1 Index*

Enter the index for the challenge password here.

**Telnet 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=HIRSCHMANN CA/O=HIRSCHMANN/C=DE`

**Telnet 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.

**Telnet 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.

**Telnet 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*

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.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

**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.

**SNMP ID:** 2.39.2.5.4

**Telnet path:** /Setup/Certificates/SCEP-CA/Client-Certificates/General-challenge-password

**Possible values:**

- Max. 16 characters

**Default:** XuL[ksKcC3+'%PA2

## 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.

**Telnet 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.

**Telnet 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.

**Telnet path:** /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists

### 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. .

**Telnet path:** /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/CRL-Update-Interval

**Possible values:**

- Max. 63 numerical characters

**Default:** 86,400

### 2.39.2.8.2 CRL-Distribution-Point-Hostname

Enter here the update interval in seconds for creating a new CRL. The lower limit for this is 600 seconds.

**Telnet path:** /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/CRL-Distribution-Point-Hostname

**Possible values:**

- Max. 63 numerical characters

**Default:** 600

### 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.

**SNMP ID:** 2.39.2.8.3

**Telnet path:** /Setup/Certificates/SCEP-CA/Certificate-Revocation-Lists/Create-New-CRL

## 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.

**SNMP ID:** 2.39.2.9

**Telnet path:** /Setup/Certificates/SCEP-CA/Reinitialize

## 2.39.2.10 Notification

This menu contains the settings for the notification of events relating to certificates.

**Telnet path:** /Setup/Certificates/SCEP-CA/Logging

### 2.39.2.10.1 E-Mail

The setting here determines whether a notification is sent when an event occurs.

**Telnet path:** /Setup/Certificates/SCEP-CA/Logging/E-Mail

**Possible values:**

- No
- Yes

**Default:** No

### 2.39.2.10.2 Syslog

This item activates the logging function based on notifications via Syslog.

**Telnet path:** /Setup/Certificates/SCEP-CA/Logging/Syslog

**Possible values:**

- No
- Yes

**Default:** No

**Note:** To make use of this function, the Syslog client in the device needs to be configured accordingly.

#### 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.

**Telnet path:** /Setup/Certificates/SCEP-CA/Logging/E-Mail

**Possible values:**

- Maximum 63 alphanumerical characters

**Default:** Blank

#### 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.

**Telnet path:** /Setup/Certificates/SCEP-CA/Logging/Send-Backup-Reminder

**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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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 HiLCOS in the menu **Setup** > **Certificates** > **SCEP-CA** > **Client-Certificates**.

**Telnet 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:

| *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 abbreviations*

| *Device* | *OID* |
|---|---|
| WLC | 1.3.6.1.5.5.7.3.18 |
| Managed AP | 1.3.6.1.5.5.7.3.19 |

*Table 18: Extended usage: Meaningful OIDs for WLAN switching*

**Sample input**: `critical,clientAuth,1.3.6.1.5.5.7.3.19`

### Telnet 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.

| *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. |

*Table 19: Usage: Abbreviation*

**Sample input**: `digitalSignature, nonRepudiation`

**Telnet 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 HiLCOS 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.

**Telnet 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

### 2.39.2.13.9 Reboot

This action causes a restart of the sub-CA. Execute this action after performing configuration changes on the sub-CA.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **Sub-CA**

**Possible arguments:**

*none*

## 2.39.2.14 Web interface

In this directory, you configure the settings for the SCEP-CA web interface.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA**

### 2.39.2.14.1 Profiles

In this table you create profiles with collected certificate properties.

**Note:** By default three profiles are already available for common application scenarios.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **Web-Interface**

#### *2.39.2.14.1.1 Profile name*

Here you assign a unique name for the profile.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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).

**Telnet 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).

**Telnet 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).

**Telnet 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).

**Telnet 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).

**Telnet 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=`.

**Telnet 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).

**Telnet 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=`.

**Telnet 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=`.

**Telnet 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**.

**Telnet 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.

**Telnet 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.

**Note:** A “Default” template is already available.

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **Web-Interface**

#### *2.39.2.14.2.1 Name*

Give the template a unique name here.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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).

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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

### 2.39.3 CRLs

This menu contains the configuration of the CRLs.

**SNMP ID:** 2.39.3

**Telnet path:** /Setup/Certificates

## 2.39.3.1 Operating

Operating: During the certificate check, the CRL (if available) will be considered as well.

**SNMP ID:** 2.39.3.1

**Telnet path:** /Setup/Certificates/CRLs

**Possible values:**

- Yes
- No

**Default:** No

**Note:** 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.

## 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.

**SNMP ID:** 2.39.3.4

**Telnet path:** /Setup/Certificates/CRLs

**Possible values:**

- Max. 10 characters

**Default:** 300

**Note:** If the first attempt to load the CRL fails, new attempts are made at regular short intervals.

## 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 retreival.

**SNMP ID:** 2.39.3.5

**Telnet path:** /Setup/Certificates/CRLs

**Possible values:**

- Max. 10 characters

**Default:** 0

**Note:** If with regular updates the CRL cannot be retreived, no further attempts will be started until the next regular attempt.

## 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.

**SNMP ID:** 2.39.3.6

**Telnet path:** /Setup/Certificates/CRLs

**Possible values:**

- Max. 10 characters

**Default:** 0

**Special values:** Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

**Note:** In the time period defined here, even expired certificates can be used to maintain or re-establish a connection.

## 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).

**SNMP ID:** 2.39.3.7

**Telnet 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 HiLCOS, 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.

**SNMP ID:** 2.39.3.8

**Telnet path:** /Setup/Certificates/CRLs/Alternative-URL-Table

### 2.39.3.8.1 Alternative-URL

Here you enter the alternative URL where a CRL can be collected.

**SNMP ID:** 2.39.3.8.1

**Telnet path:** /Setup/Certificates/CRLs/Alternative-URL-Table/Alternative-URL

**Possible values:**

- Any valid URL with max. 251 characters.

**Default:** Blank

### 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.

**SNMP ID:** 2.39.3.9

**Telnet path:** /Setup/Certificates/CRLs/Loopback-Address

**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
- LB0 – LBF for the 16 loopback addresses
- Any valid IP address

**Default:** Blank

**Note:** If there is an interface called "DMZ", its address will be taken if you have selected "DMZ".

## 2.40 GPS

This item contains the GPS settings.

**SNMP ID:** 2.40

**Telnet path:** /Setup/GPS

### 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.

**Telnet path:**

**Setup** > **GPS**

**Possible values:**

No

Yes

**Default:**

No

# 2.51 HiDiscovery

This menu contains the values for the HiDiscovery protocol configuration.

**Telnet path:** Setup

## 2.51.1 Server-Operating

This parameter enables or disables the use of the HiDiscovery protocol.

**Telnet path:** Setup/HiDiscovery

**Possible values:**

- Disabled
- Read-Only
- Enabled

**Default:** Disabled

# 2.52 COM-Ports

This menu contains the configuration of the COM ports.

**SNMP ID:** 2.52

**Telnet 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.

**SNMP ID:** 2.52.1

**Telnet path:** /Setup/COM-Ports

## 2.52.1.1 Device-Type

Selects a serial interface from the list of those available in the device.

**SNMP ID:** 2.52.1.1

**Telnet path:** /Setup/COM-Ports/Devices

**Possible values:**

- All available serial interfaces.

**Default:** Outband

## 2.52.1.4 Service

Activation of the port in the COM port server.

**SNMP ID:** 2.52.1.4

**Telnet path:** /Setup/COM-Ports/Devices

**Possible values:**

- WAN
- COM-port server

**Default:** WAN

### 2.52.2 COM-Port-Server

This menu contains the configuration of the COM-port server.

**SNMP ID:** 2.52.2

**Telnet path:** /Setup/COM-Ports

## 2.52.2.1 Operational

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.

**SNMP ID:** 2.52.2.1

**Telnet 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.

**SNMP ID:** 2.52.2.1.1

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Possible values:**

- All available serial interfaces.

**Default:** Outband

### 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.

**SNMP ID:** 2.52.2.1.2

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.52.2.1.4

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Device-Type

**Possible values:**

- Yes
- No

**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.

**SNMP ID:** 2.52.2.2

**Telnet 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.

**SNMP ID:** 2.52.2.2.1

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

**Possible values:**

- All available serial interfaces.

**Default:** Outband

### 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.

**SNMP ID:** 2.52.2.2.2

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

**Possible values:**

- Max. 10 characters

**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

**SNMP ID:** 2.52.2.2.4

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

**Possible values:**

- 110 to 230400

**Default:** 9600

#### 2.52.2.2.5 Data-Bits

Number of data bits.

**SNMP ID:** 2.52.2.2.5

**Telnet 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.

**SNMP ID:** 2.52.2.2.6

**Telnet 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.

**SNMP ID:** 2.52.2.2.7

**Telnet 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.

**SNMP ID:** 2.52.2.2.8

**Telnet 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 status 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" status.

**SNMP ID:** 2.52.2.2.9

**Telnet 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.

**SNMP ID:** 2.52.2.2.10

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/COM-Port-Settings

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.52.2.3

**Telnet path:** /Setup/COM-Ports/COM-Port-Server

#### 2.52.2.3.1 Device-Type

Selects a serial interface from the list of those available in the device.

**SNMP ID:** 2.52.2.3.1

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- All available serial interfaces.

**Default:** Outband

#### 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.

**SNMP ID:** 2.52.2.3.2

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.52.2.3.4

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Servers
- Client

**Default:** Servers

#### 2.52.2.3.5 Listen-Port

The TCP port where the COM port in TCP server mode expects incoming connections.

**SNMP ID:** 2.52.2.3.5

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.52.2.3.6

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- DNS-Name
- IP address

**Default:** Blank

#### 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.

**SNMP ID:** 2.52.2.3.7

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Max. 10 characters

**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.

**SNMP ID:** 2.52.2.3.8

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Max. 16 characters

**Default:** Blank

#### 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.

**SNMP ID:** 2.52.2.3.9

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Yes
- No

**Default:** Yes

### 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.

**SNMP ID:** 2.52.2.3.10

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- CRLF
- CR
- LF

**Default:**

CRLF

**Note:** This setting is only relevant if binary mode is deactivated for this port.

### 2.52.2.3.12 TCP-Retransmit-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.

**SNMP ID:** 2.52.2.3.12

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- 0 to 99 seconds
- Maximum 2 characters

**Special values:**

- 0 activates the RFC 1122 default value (60 seconds).

**Default:**

- 0

**Note:** 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.

### 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.

**SNMP ID:** 2.52.2.3.13

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- 0 to 9
- Maximum 1 characters

**Special values:**

- 0 activates the RFC 1122 default value (5 attempts).

**Default:**

- 0

**Note:** 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.

### 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.

**SNMP ID:** 2.52.2.3.14

**Telnet 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:**

- Down

**Note:** The setting "active" is recommended for server applications.

### 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.).

**SNMP ID:** 2.52.2.3.15

**Telnet path:** /Setup/COM-Ports/COM-Port-Server/Network-Settings

**Possible values:**

- Maximum 10 characters.

**Default:**

- 0

**Special values:**

- 0 activates 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**.

**Telnet 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).

**SNMP ID:** 2.52.3

**Telnet 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.

**SNMP ID:** 2.52.3.1

**Telnet path:** /Setup/COM-Ports/WAN

### 2.52.3.1.1 Device-Type

List of serial interfaces available in the device.

**SNMP ID:** 2.52.3.1.1

**Telnet path:** /Setup/COM-Ports/WAN/Devices

**Possible values:**

- All available serial interfaces.

### 2.52.3.1.3 Operating

Status of connected device.

**SNMP ID:** 2.52.3.1.3

**Telnet path:** /Setup/COM-Ports/WAN/Devices

**Possible values:**

- Yes
- No

## 2.52.4 Serial configuration

This menu contains the settings for the auto configuration of WLAN point-to-point links over a serial connection.

**Telnet path:** /Setup/COM-Ports

### 2.52.4.1 Bit rate

This item sets the bit rate for communications between the devices when a serial connection is used for the automatic configuration of WLAN point-to-point links.

**Telnet path:** /Setup/COM-Ports

**Possible values:**

- 1200
- 2400
- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

**Default:** 9600

**Note:** It is imperative that the same bit rate is set in all devices communicating over serial connections to be used for the automatic configuration of WLAN point-to-point links.

## 2.53 Temperature-Monitor

The settings for the temperature monitor are located here.

**SNMP ID:** 2.53

**Telnet path:** /Setup/Temperature-Monitor

### 2.53.1 Upper-Limit-Degrees

When the temperature set here is exceeded, the device sends an SNMP trap of the type "trpTempMonOverTemp".

**Telnet path:**/Setup/Temperature-Monitor/Upper-Limit-Degrees

**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".

**Telnet path:**/Setup/Temperature-Monitor/Upper-Limit-Degrees

**Possible values**:

- 0 – 127 ° Celsius

**Default**: 0

## 2.54 TACACS

### 2.54.2 Authorization

**WEBconfig:** /Setup/Tacacs+

**WEBconfig English:** /Setup/Tacacs+

Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

**Possible values**: Activated, deactivated

**Default**: Deactivated

**Note:** 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.

### 2.54.3 Accounting

**WEBconfig:** /Setup/Tacacs+

Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values: Activated, deactivated

Default: Deactivated

**Note:** TACACS+ accounting will only activate if the defined TACACS+ server is available.

### 2.54.6 Shared-Secret

**WEBconfig:** /Setup/Tacacs+

The password for encrypting the communications between NAS and TACACS+ servers.

**Possible values:** 31 alphanumerical characters

**Default:** Blank

**Note:** The password must be entered identically into the device and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

### 2.54.7 Encryption

**WEBconfig:** /Setup/Tacacs+

**WEBconfig English:** /Setup/Tacacs+

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

**Possible values:**

- Activated
- Disabled

**Default:** Activated

**Note:** 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.

### 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.

**SNMP ID:** 2.54.9

**Telnet path:** /Setup/Tacacs+

## 2.54.9.1 Server-address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

**SNMP ID:** 2.54.9.1

**Telnet path:** /Setup/Tacacs+/Server-Address

**Possible Telnet values:**

- Valid DNS resolvable name or valid IP address.

**Default:** Blank

## 2.54.9.2 Loopback-Address

Optionally you can configure a loopback address here.

**SNMP ID:** 2.54.9.2

**Telnet path:** /Setup/Tacacs+/Loopback-Address

**Possible Telnet 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:** Blank

### 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.

**SNMP ID:** 2.54.9.3

**Telnet path:** /Setup/Tacacs+/Compatibility-Mode

**Possible Telnet values:**

- Activated
- Disabled

**Default**: Deactivated

## 2.54.10 Fallback to local users

**WEBconfig:** /Setup/Tacacs+

**WEBconfig English:** /Setup/Tacacs+

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.

**Possible values:** Allowed, prohibited

**Default:** Allowed

**Note:** 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.

## 2.54.11 SNMP-GET-Requests-Authorisation

**WEBconfig:** /Setup/Tacacs+

**WEBconfig English:** /Setup/Tacacs+

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.

**Possible values:**

- only_for_SETUP_tree: With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of HiLCOS.
- 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

## 2.54.11 SNMP-GET-Requests-Accounting

**WEBconfig:** /Setup/Tacacs+

**WEBconfig English:** /Setup/Tacacs+

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.

**Note:** 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.

**Possible values:**

- only_for_SETUP_tree: With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of HiLCOS.
- 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.

**SNMP ID:** 2.54.13

**Telnet path:** /Setup/Tacacs+

**Possible values:**

- Activated
- Disabled

**Default**: Deactivated

**Note:** 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!

### 2.54.14 Include-value-into-authorisation-request

If you deactivate this function, then TACACS + only checks the rights of the user on login. When entering values, the device no longer checks whether the user has permission to change certain values.

**Telnet path:**/Setup/Tacacs+/Include-value-into-authorization

**Possible values:**

- Activated: When values are submitted, TACACS + checks whether the user has the right to make these changes
- Deactivated: TACACS + checks the identity of the user only on login

**Default:** Activated

## 2.59 WLAN-Management

This menu is used to configure the WLAN management.

### 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.

**SNMP ID:** 2.59.1

**Telnet path:** /Setup/WLAN-Management/Static-WLC-Configuration

### 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.

**SNMP ID:** 2.59.1.1

**Telnet path:** /Setup/WLAN-Management/Static-WLC-Configuration/IP-Address

**Possible values:**

- Valid IP address or resolvable name of a WLC controller

**Default:** WLC-Address

## 2.59.1.2 Port

The port to be used for communication with the WLAN controller is set here.

**SNMP ID:** 2.59.1.2

**Telnet path:** /Setup/WLAN-Management/Static-WLC-Configuration/Port

**Possible values:**

- Valid port name

**Default:** 1027

## 2.59.1.3 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.

**SNMP ID:** 2.59.1.3

**Telnet path:** /Setup/WLAN-Management/Static-WLC-Configuration/Loopback-Address

**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 (Note: If there is an interface named "DMZ", its address will be taken).
- LB0 ... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

**Default:** Blank

**Note:** The sender address specified here is used **unmasked** for every remote station.

### 2.59.3 CAPWAP-Tuning

Here you can configure the CAPWAP timing parameters (CAPWAP Tuning).

**Telnet path:**

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

## 2.59.3.1 Echo-Interval

Here you specify the duration of the Echo Interval in seconds.

The Echo Interval is the time interval between the AP sends Echo Request messages to the controller with which the AP has joined.

**Telnet path:**

**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**

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

**Default:**

10

## 2.59.3.2 Retransmit-Interval

Here you specify the duration of the Retransmit Interval in seconds.

The Retransmit Interval is the time interval in which a non-ackowledged CAPWAP packet will be retransmitted.

**Telnet path:**

**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**

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

**Default:**

3

## 2.59.3.3 Discovery-Interval

Here you specify the duration of the Discovery Interval in seconds.

The Discovery Interval is the time interval in which the AP waits for more Discovery Responses after receiving the first Discovery Response.

**Telnet path:**

**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**

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

**Default:**

5

## 2.59.3.4 Max-Discovery-Interval

Here you specify the duration of the Maximum Discovery Interval in seconds.

The Maximum Discovery Interval is the maximum time interval allowed between sending Discovery Request messages.

**Telnet path:**
**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**
Max. 5 characters from `[0-9]`

**Default:**
8

## 2.59.3.5 Silent-Interval

Here you specify the duration of the Silent Interval in seconds.

The Silent Interval is the time interval an AP must wait before it may send Discovery Request messages or attempt to establish a DTLS session.

**Telnet path:**
**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**
Max. 5 characters from `[0-9]`

**Default:**
2

## 2.59.3.6 Enable

Here you enable or disable the CAPWAP Tuning.

**Telnet path:**
**Setup** > **WLAN-Management** > **CAPWAP-Tuning**

**Possible values:**

**No**

CAPWAP Tuning disabled

**Yes**

CAPWAP Tuning enabled

**Default:**

No

## 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.

**Note:** 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).

**Telnet 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.

**Note:** If AutoWDS for your device is set to the property "Activate express integration as fallback setting" along with the product code, the presetting changes to **Yes**.

**Telnet 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.

**Important:** 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`.

**Telnet 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.

**Important:** 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`.

**Telnet 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* .

**Important:** 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`.

**Telnet 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.

**Telnet 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.

**Telnet path:**

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

**Possible values:**

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

0 … 65535

**Default:**

1027

## 2.59.120 Log-Entries

This parameter defines the maximum number of log entries for the device.

**Telnet path:**/Setup/WLAN-Management/Log-Entries

**Possible values:**

- 0 to 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.

**SNMP ID:** 2.60

**Telnet path:** /Setup/Autoload

## 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.

**SNMP ID:** 2.60.1

**Telnet path:** /Setup/Autoload/Network

**Note:** 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.

**Note:** 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.

## 2.60.1.1 Firmware

This menu is used to configure the automatic uploading of firmware over the network.

**SNMP ID:** 2.60.1.1

**Telnet path:** /Setup/Autoload/Network/Firmware

### 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.

**SNMP ID:** 2.60.1.1.1

**Telnet 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

**Note:** If the command LoadFirmware is executed twice in succession with the setting "unconditionally", both memory locations will contain the same firmware version.

#### 2.60.1.1.2 Minimum-Version

Specify the minimum version of the firmware to be loaded over the network.

**SNMP ID:** 2.60.1.1.2

**Telnet path:** /Setup/Autoload/Network/Minimum-Version

**Possible values:**

- Max. 14 characters

**Default:** Blank

**Note:** Firmware versions with a lower version number will be ignored.

#### 2.60.1.1.3 URL

Specify the URL of the firmware that is to be uploaded over the network using the LoadFirmware command.

**SNMP ID:** 2.60.1.1.3

**Telnet path:** /Setup/Autoload/Network/Firmware/URL

**Possible values:**

- Max. 127 characters beginning with "tftp://", "http://" or "https://"

**Default:** Blank

**Note:** 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.

## 2.60.1.2 Configuration

This menu contains the settings for uploading a configuration over the network.

**SNMP ID:** 2.60.1.2

**Telnet path:** /Setup/Autoload/Network/Configuration

### 2.60.1.2.1 Condition

This is where you select the condition under which the configuration specified under /Setup/Autoload/Network/Configuration/URL will be uploaded when the device is started.

**SNMP ID:** 2.60.1.2.1

**Telnet path:** /Setup/Autoload/Network/Configuration

**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.

**Telnet path:**

**Setup** > **Autoload** > **Network** > **Config**

**Possible values:**

Any valid URL with max. 127 characters.

**Default:**

## 2.60.1.3 Script

This menu contains the settings for uploading a script over the network.

**SNMP ID:** 2.60.1.3

**Telnet path:** /Setup/Autoload/Network/Script

#### 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.

**SNMP ID:** 2.60.1.3.1

**Telnet 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.

**Telnet path:**

**Setup** > **Autoload** > **Network** > **Script**

**Possible values:**

Any valid URL with max. 127 characters.

**Default:**

### 2.60.1.4 TFTP-Client

This menu contains the configuration for the TFTP client.

**SNMP ID:** 2.60.1.4

**Telnet path:** /Setup/Autoload/Network/TFTP-Client

#### 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.

**SNMP ID:** 2.60.1.4.1

**Telnet path:** /Setup/Autoload/Network/TFTP-Client

**Possible values:**

- 4 characters

**Default:** 8192

**Note:** 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.

### 2.60.56 USB

This menu is used to configure the automatic uploading of firmware or configurations from external data media.

**SNMP ID:** 2.60.56

**Telnet path:** /Setup/Autoload/USB

### 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.

**SNMP ID:** 2.60.56.1

**Telnet path:** /Setup/Autoload/USB

**Possible values:**

- Inactive: Automatic loading of loader and/or firmware files is deactivated.
- Active: 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

**Note:** This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

## 2.60.56.2 Config-and-script

This option activates the automatic loading of configuration and/or script files from a connected USB medium. Save the required configuration and/or script files in the "Config" directory located in the root directory of the connected USB media.

**SNMP ID:** 2.60.56.2

**Telnet path:** /Setup/Autoload/USB

**Possible values:**

- Inactive: Automatic loading of configuration and/or script files is deactivated.
- Active: 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

**Note:** This option is set to "inactive" in the Security Settings Wizard or the Basic Settings Wizard.

**Note:** 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.

# 2.63 Packet-Capture

This menu contains the settings for recording network data traffic via LCOScap and RPCAP.

**Telnet path:**

**Setup** > **Packet-Capture**

## 2.63.1 LCOSCap-Operating

This setting activates the LCOSCAP function.

**Telnet path:**

**Setup** > **Packet-Capture** > **LCOSCap-Operating**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.63.2 LCOSCap-Port

This setting specifies the port used by LCOSCAP.

**Telnet path:**

**Setup** > **Packet-Capture** > **LCOSCap-Port**

**Possible values:**

5 characters from ‘0123456789’

**Default:**

41047

## 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".

**Telnet path:**

**Setup** > **Packet-Capture**

**Possible values:**

Yes

No

**Default:**

No

## 2.63.12 RPCap-Port

This setting specifies the port used by RPCAP.

**Telnet path:**

**Setup** > **Packet-Capture**

**Possible values:**

0 to 65535

**Default:**

2002

# 2.70 IPv6

This menu contains the settings for IPv6.

**Telnet path:**

**Setup** > **IPv6**

## 2.70.1 Tunnel

Use this setting to manage the tunneling protocols to provide access to the IPv6 Internet via an IPv4 Internet connection.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel**

## 2.70.1.1 6in4

The table contains the settings for the 6in4 tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4**

### 2.70.1.1.1 Peer name

Contains the name of the 6in4 tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Peer-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 0 – 65534

**Default:**

0

#### 2.70.1.1.3 Gateway-Address

Contains the IPv4 address of the remote 6in4 gateway.

**Note:** The 6in4 tunnel is only set up if the gateway can be reached by ping at this address.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Gateway-Address**

**Possible values:**

IP address in IPv4 notation, max. 64 characters

**Default:**

Blank

#### 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

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **IPv4-Rtg-tag**

**Possible values:**

Max. 5 characters in the range 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".

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Gateway-IPv6-Address**

**Possible values:**

IPv6 address with max. 43 characters

**Default:**

Blank

### 2.70.1.1.6 Lokale-IPv6-Address

Contains the local IPv6 address of the device on the intermediate network, for example "2001:db8::2/64".

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Local-IPv6-Address**

**Possible values:**

Max. 43 characters

**Default:**

Blank

#### 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".

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Routed-IPv6-Prefix**

**Possible values:**

Max. 43 characters

**Default:**

Blank

#### 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** .

**Note:** Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6in4** > **Firewall**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay**

### 2.70.1.2.1 Peer name

Contains the name of the 6rd border relay tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Peer-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **IPv4-Loopback-Address**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **6rd-Prefix**

**Possible values:**

Max. 24 characters as a prefix of an IPv6 address with up to four blocks of four hexadecimal digits each

**Default:**

Blank

#### 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 |

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **IPv4-Mask-Length**

**Possible values:**

Max. 2 numbers in the range 0 – 32

**Default:**

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.

**Note:** If you do not enable this feature, you must manually configure the required 6rd settings for the 6rd clients.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **DHCPv4-Propagate**

**Possible values:**

Yes

No

**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** .

**Note:** Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Firewall**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.1.3 6rd

The table contains the settings for the 6rd tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd**

### 2.70.1.3.1 Peer name

Contains the name of the 6rd tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd** > **Peer-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 0 – 65534

**Default:**

0

#### 2.70.1.3.3 Border-Relay-Address

Contains the IPv4 address of the 6rd-border relay.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd4** > **Border-Relay-Address**

**Possible values:**

IPv4 address with max. 64 characters

**Default:**

Blank

#### 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

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd** > **IPv4-Rtg-tag**

**Possible values:**

Max. 5 characters in the range 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.

**Note:** If the 6rd prefix is assigned through DHCPv4, you have to enter "::/32" here.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd** > **6rd-Prefix**

**Possible values:**

Max. 24 characters

**Default:**

Blank

### 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 |

| *6rd domain* | *Mask length* | *6rd prefix* |
|---|---|---|
| 2001:db8:2:3300::/56 | 24 | 2001:db8:2:3363::/64 |

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd** > **IPv4-Mask-Length**

**Possible values:**

Max. 2 numbers in the range 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** .

**Note:** Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6rd4** > **Firewall**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.70.1.4 6to4

The table contains the settings for the 6to4 tunnel.

**Note:** 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6to4**

#### 2.70.1.4.1 Peer name

Contains the name of the 6to4 tunnel.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6to4** > **Peer-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6to4** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 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.

**Note:** The 6to4 tunnel is only set up if the gateway can be reached by ping at this address.

#### Telnet path:

**Setup** > **IPv6** > **Tunnel** > **6to4** > **Gateway-Address**

#### Possible values:

IPv4 address with max. 64 characters

#### 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

#### Telnet path:

**Setup** > **IPv6** > **Tunnel** > **6to4** > **IPv4-Rtg-tag**

#### Possible values:

Max. 5 characters in the range 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** .

**Note:** Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

**Telnet path:**

**Setup** > **IPv6** > **Tunnel** > **6to4** > **Firewall**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement**

## 2.70.2.1 Prefix-Optionen

The table contains the settings for IPv6 prefixes for each interface.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

#### 2.70.2.1.1 Interface-Name

Defines the name of the logical interface.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 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).

**Note:** 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**.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 43 characters

**Default:**

Blank

### 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").

**Note:** 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 19 characters

**Default:**

1

#### 2.70.2.1.4 Adv.-OnLink

Indicates whether the prefix is "on link".

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Yes

No

**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).

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 2.70.2.1.7 Adv.-Pref.-Lifetime

Defines the time in milliseconds 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 10 numbers in the range 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Max. 10 numbers in the range 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Options**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.2.2 Interface-Options

The table contains the settings for the IPv6 interfaces.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Interface-Options**

### 2.70.2.2.1 Interface-Name

Defines the name of the logical interface to be used for sending router advertisements.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 2.70.2.2.2 Send-Adverts

Enables the periodic transmission of router advertisements and the response to router solicitations.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Send-Adverts**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Min-RTR-Interval**

**Possible values:**

Min. 3 seconds

Max. 0.75 * **Max-RTR-Interval**

Max. 10 numbers

**Default:**

0.33 * **Max-RTR-Interval** (if **Max-RTR-Interval** >= 9 seconds)

**Max-RTR-Interval** (if **Max-RTR-Interval** < 9 seconds)

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Max-RTR-Interval**

**Possible values:**

Min. 4 seconds

Max. 1800 seconds

Max. 10 numbers

**Default:**

600 seconds

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Managed-Flag**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Other-Config-Flag**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.70.2.2.7 Link-MTU

Here you set the valid MTU for the corresponding link.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Link-MTU**

**Possible values:**

Max. 5 numbers in the range 0 – 99999

**Default:**

1500

### 2.70.2.2.8 Reachable-Time

Specifies the time in seconds 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Reachable-Time**

**Possible values:**

Max. 10 numbers in the range 0 – 2147483647

**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".

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Hop-Limit**

**Possible values:**

Max. 5 numbers in the range 0 – 255

**Default:**

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.

**Note:** If this value is set to **0**, the operating system will not use this router as the default router.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Def.-Lifetime**

**Possible values:**

Max. 10 numbers in the range 0 – 2147483647

**Default:**

1800

### 2.70.2.2.12 Default-Router-Mode

Defines how the device advertises itself as the default gateway or router.

The settings have the following functions:

- **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".

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Default-Router-Modus**

**Possible values:**

Auto

Always

Never

**Default:**

Auto

### 2.70.2.2.13 Router-Preference

Defines the preference of this router. Clients enter this preference into their local routing tables.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **Interface-Options** > **Router-Preference**

**Possible values:**

Low

Medium

High

**Default:**

Medium

### 2.70.2.2.14 RTR-Time

Specifies the time in seconds between successive transmissions of neighbor-solicitation messages to a neighbor if the address is being resolved or the accessibility is being tested.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Interface-Options**

**Possible values:**

0 to 4294967295

**Default:**

0

## 2.70.2.3 Route-Options

The table contains the settings for the route options.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Route-Options**

### 2.70.2.3.1 Interface-Name

Defines the name of the interface that this route option applies to.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Route-Options** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Route-Options** > **Prefix**

**Possible values:**

IPv6 prefix with max. 43 characters, e.g. 2001:db8::/64

**Default:**

Blank

#### 2.70.2.3.3 Route-Lifetime

Set how long in seconds the route should remain valid.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Route-Options** > **Route-Lifetime**

**Possible values:**

Max. 5 numbers in the range 0 – 65335

**Default:**

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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement** > **Route-Options** > **Route-Preference**

**Possible values:**

Low

Medium

High

**Default:**

Medium

### 2.70.2.5 RDNSS-Options

This table contains the settings of RDNSS extension (recursive DNS server).

**Note:** This function is not currently supported by Windows. Propagation of a DNS server, where required, is performed via DHCPv6.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **RDNSS-Options**

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **RDNSS-Options**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 2.70.2.5.2 Primary-DNS

IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC6106) for this interface.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **RDNSS-Options**

**Possible values:**

Valid IPv6 address

**Default:**

Blank

### 2.70.2.5.3 Secondary-DNS

IPv6 address of the secondary IPv6 DNS server for this interface.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **RDNSS-Options**

**Possible values:**

Valid IPv6 address

**Default:**

Blank

### 2.70.2.5.4 DNS-Search-List

This parameter defines which DNS search list the device propagates on this logical network.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **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 enabled, WAN disabled.

### 2.70.2.5.5 Lifetime

Defines the time in seconds for which a client may use this DNS server for name resolution.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisements** > **RDNSS-Options**

**Possible values:**

- Max. 5 numbers in the range 0 – 65535
- 0: Discontinuation

**Default:**

900

## 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**.

**Telnet path:**

**Setup** > **IPv6** > **Router-Advertisement**

### 2.70.2.6.1 Interface name

Specify the name of the RAS interface applicable for this prefix pool.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Attention:** 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.

**Telnet 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".

**Telnet 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).

**Telnet 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 milliseconds 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.

**Telnet 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.

**Telnet path:**
**Setup** > **IPv6** > **Router-Advertisement** > **Prefix-Pools**

**Possible values:**
Max. 10 characters from `0123456789`

**Default:**

2592000

## 2.70.3 DHCPv6

This menu contains the DHCPv6 settings.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6**

## 2.70.3.1 Server

This menu contains the DHCP server settings for IPv6.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server**

### 2.70.3.1.2 Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pool**

#### *2.70.3.1.2.1 Address pool name*

Specify the name of the address pool here.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools** > **Address-Pool-Name**

**Possible values:**

Maximum 31 characters

**Default:**

Blank

#### *2.70.3.1.2.2 Start-Address-Pool*

Here you specify the first address in the pool, e.g. "2001:db8::1"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools** > **Start-Address-Pool**

**Possible values:**

Maximum 39 characters

**Default:**

Blank

#### *2.70.3.1.2.3 End-Address-Pool*

Here you specify the last address in the pool, e.g. "2001:db8::9"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools** > **End-Address-Pool**

**Possible values:**

Maximum 39 characters

**Default:**

Blank

#### *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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools** > **Pref.-Lifetime**

**Possible values:**

Maximum 10 characters.

**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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools** > **Valid-Lifetime**

**Possible values:**

Maximum 10 characters.

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**

**Possible values:**

Maximum 16 characters

**Default:**

Blank

### 2.70.3.1.3 PD-Pools

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

#### *2.70.3.1.3.1 PD-Pool-Name*

Specify the name of the PD pool here.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **PD-Pool-Name**

**Possible values:**

Maximum 31 characters

**Default:**

Blank

#### *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::"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Start-PD-Pool**

**Possible values:**

Maximum 39 characters

**Default:**

Blank

#### *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::"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **End-PD-Pool**

**Possible values:**

Maximum 39 characters

**Default:**

Blank

#### 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"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Prefix-Length**

**Possible values:**

Maximum 3 characters.

**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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Pref.-Lifetime**

**Possible values:**

Maximum 10 characters.

**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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Valid-Lifetime**

**Possible values:**

Maximum 10 characters.

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

**Possible values:**

Maximum 16 characters

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

#### *2.70.3.1.4.1 Interface-Name-or-Relay*

Name of the interface on which the DHCPv6 server is working, for example "INTRANET"

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List** > **Interface-Name**

**Possible values:**

Selection from the list of LAN interfaces defined in the device; max. 39 characters

**Default:**

Blank

#### *2.70.3.1.4.2 Operating*

Activates or deactivates the DHCPv6 server.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List** > **Operating**

**Possible values:**

No

Yes

**Default:**

Yes

#### *2.70.3.1.4.3 Primary-DNS*

IPv6 address of the primary DNS server.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List** > **Primary-DNS**

**Possible values:**

IPv6 address with max. 39 characters

**Default:**

::

#### *2.70.3.1.4.4 Secondary-DNS*

IPv6 address of the secondary DNS server.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List** > **Secondary-DNS**

**Possible values:**

IPv6 address with max. 39 characters

**Default:**

Blank

#### *2.70.3.1.4.5 Address-Pool-Name*

Here you specify the address pool that the devices uses for this interface.

**Note:** If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the table **Setup** > **IPv6** > **DHCPv6** > **Server** > **Address-Pools**.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Address-Pool-Name**

**Possible values:**

Maximum 31 characters

**Default:**

Blank

#### *2.70.3.1.4.6 PD-Pool-Name*

Specify the prefix-delegation pool that the devices is to use for this interface.

**Note:** 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**.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **PD-Pool-Name**

**Possible values:**

Maximum 31 characters

**Default:**

Blank

#### 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.

**Note:** The client must explicitly include the rapid commit option in its solicit message.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Rapid-Commit**

**Possible values:**

No

Yes

**Default:**

No

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Preference**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

**Possible values:**

0 to 255

**Default:**

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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

**Possible values:**

0 to 255

**Default:**

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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

**Possible values:**

Valid Unicast address

**Default:**

Blank

#### 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.

**Telnet 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 own domain can be configured under IPv4 > 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 (Deutsche Telekom Privacy feature), 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Interface-List**

**Possible values:**

**Off**: Disables the reconfigure function

**Prohibit**: 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.

**Note:** This parameter is only required for development tests and is not relevant for normal operations. Never change this default setting!

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server**

**Possible values:**

Yes

No

**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.

**Telnet 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Selection from the list of LAN interfaces defined in the device; max. 39 characters

**Default:**

Blank

##### *2.70.3.1.6.2 Address or PD prefix*

IPv6 address or PD prefix that you want to assign statically.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Maximum 43 characters

**Default:**

Blank

##### *2.70.3.1.6.3 Client-ID*

DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `show dhcpv6-client` or in WEBconfig under **Status** > **IPv6** > **DHCPv6** > **Client** > **Client ID**.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under **Status** > **IPv6** > **DHCPv6** > **Server** > **Address bindings**, and retrieved IPv6 prefixes are under **Status** > **IPv6** > **DHCPv6** > **Server** > **PD bindings**.

LANmonitor displays that client IDs under **DHCPv6 server**.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Maximum 96 characters

**Default:**

Blank

#### *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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Maximum 10 characters.

**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".

**Note:** 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Maximum 10 characters.

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

Maximum 16 characters

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server**

**Possible values:**

**No**
**Yes**

**Default:**

No

## 2.70.3.2 Client

This menu contains the DHCP client settings for IPv6.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client**

### 2.70.3.2.1 Interface-Liste

This table determines the behavior of the DHCPv6 client.

**Note:** Normally client behavior is controlled by the auto-configuration.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

#### *2.70.3.2.1.1 Interface-Name*

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".

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Interface-Name**

**Possible values:**

Selection from the list of LAN interfaces defined in the device; max. 16 characters

**Default:**

Blank

#### *2.70.3.2.1.2 Operating*

Here you specify if and how the device enables the client. Possible values are:

- **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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Operating**

**Possible values:**

Autoconf

No

Yes

**Default:**

Autoconf

#### *2.70.3.2.1.3 Request-DNS*

Here you specify whether the client should query the DHCPv6 server for DNS servers.

**Note:** You must enable this option in order for the device to obtain information about a DNS server.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Request-DNS**

**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.

**Note:** Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i.e. not distributed by 'SLAAC'.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Request-Address**

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Request-PD**

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List** > **Rapid-Commit**

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

**Possible values:**

Yes

No

**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.

**Note:** In order for dynamic reconfiguration to work, you also have to enable it on the server!

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

**Possible values:**

Yes

No

**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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

**Possible values:**

Yes

No

**Default:**

Yes

### 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **User-Class-Identifier**

**Possible values:**

Maximum 253 characters

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Vendor-Class-Identifier**

**Possible values:**

Maximum 253 characters

**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).

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client**

**Possible values:**

Maximum 10 characters

**Default:**

2356

## 2.70.3.3 Relay-Agent

This menu contains the DHCP relay agent settings for IPv6.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Relay-Agent**

### 2.70.3.3.1 Interface-Liste

This table determines the behavior of the DHCPv6 relay agent.

**Telnet path:**

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

#### *2.70.3.3.1.1 Interface-Name*

Define the name of the interface on which the relay agent receives requests from DHCPv6 clients, e.g. "INTRANET".

**Telnet path:**

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

**Possible values:**

Selection from the list of LAN interfaces defined in the device; max. 16 characters

**Default:**

Blank

#### *2.70.3.3.1.2 Relay agent operating*

With this option you define if and how the device enables the relay agent.

**Telnet path:**

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

**Possible values:**

**Yes:** Relay agent is enabled. This option is the default setting.

**No:** Relay agent is not 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.

**Telnet path:**

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

**Possible values:**

Maximum 39 characters

**Default:**

Blank

#### *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.

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-List** > **Dest-Address**

**Possible values:**

Maximum 39 characters

**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.

**Telnet path:**

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

**Possible values:**

Maximum 39 characters

**Default:**

Blank

### 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IPv6** > **Network**

## 2.70.4.1 Addresses

This table is used to manage the IPv6 addresses.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses**

### 2.70.4.1.1 Interface-Name

Give a name to the interface that you want to assign the IPv6 network.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

### 2.70.4.1.2 IPv6-Address-Prefixlength

Specify an IPv6 address including the prefix length for this interface.

**Note:** 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.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses** > **IPv6-Address-Prefixlength**

**Possible values:**

Max. 43 characters

**Default:**

Blank

#### 2.70.4.1.3 Address type

Specify the type of IPv6 address.

Using the address type **EUI-64** causes IPv6 addresses to be 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".

**Note:** "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".

**Note:** The prefix length for "EUI-64" must be "/64".

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses** > **Address-Type**

**Possible values:**

Unicast

Anycast

EUI-64

**Default:**

Unicast

#### 2.70.4.1.4 Name

Enter a descriptive name for this combination of IPv6 address and prefix.

**Note:** Entering a name is optional.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses** > **Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 2.70.4.1.5 Comment

Enter a descriptive comment for this entry.

**Note:** Entering a comment is optional.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Addresses** > **Comment**

**Possible values:**

Max. 64 characters

**Default:**

Blank

### 2.70.4.2 Parameter

This table is used to manage the IPv6 parameters.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Parameter**

#### 2.70.4.2.1 Interface-Name

Give a name to the interface for which the IPv6 parameters are to be configured.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Parameter** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

#### 2.70.4.2.2 IPv6-Gateway

Specify the IPv6 gateway to be used by this interface.

**Note:** This parameter overrides gateway information that the device may receive via router advertisements, for example.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Parameter** > **IPv6-Gateway**

**Possible values:**

- Global unicast address, e.g. 2001:db8::1
- Link-local address to which you add to the corresponding interface (%<INTERFACE>), e.g. fe80::1%INTERNET

**Default:**

::

#### 2.70.4.2.3 Primary-DNS

Specify the primary IPv6 DNS server to be used by this interface.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Parameter** > **Primary-DNS**

**Possible values:**

IPv6 address with max. 39 characters

**Default:**

::

#### 2.70.4.2.4 Secondary-DNS

Specify the secondary IPv6 DNS server to be used by this interface.

**Telnet path:**

**Setup** > **IPv6** > **Network** > **Parameter** > **Secondary-DNS**

**Possible values:**

IPv6 address with max. 39 characters

**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.

**Telnet path:**

**Setup** > **IPv6** > **Network**

#### 2.70.4.3.1 Name

Enter a unique name for this loopback address.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall**

## 2.70.5.1 Operating

Enables or disables the firewall.

**Note:** 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Operating**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.5.2 Forwarding-Rules

This table contains the rules that the firewall will apply for forwarding data.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

### 2.70.5.2.1 Name

Defines the name for the forwarding rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.2.2 Flags

These options determine how the firewall handles the rule. The options have the following meanings:

- **Deactivated**: 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.

You can select several options at the same time.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Disabled

Linked

Stateless

**Default:**

No selection

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Max. 4 characters from 1234567890

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Max. 5 characters from 1234567890

**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 IPv** > **IPv6** > **Firewall** > **Actions**. In addition, you can also define your own actions.

You can enter multiple actions, separated by commas.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**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 services separated by commas.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**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 stations separated by commas.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

**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 stations separated by commas.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

**Default:**

ANYHOST

#### 2.70.5.2.10 Comment

Enter a descriptive comment for this entry.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Forwarding-Rules**

**Possible values:**

0 to 65535

**Comment**

- 65535: The firewall rule is applied if the expected interface- or routing tag is 0.
- 1…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).

**Default:**

0

### 2.70.5.3 Action-List

In this table, you can group actions. Define the actions you previously under **Setup** > **IPv6** > **Firewall** > **Actions**.

**Note:** You can not delete an action in this list if the firewall is used in a forwarding or inbound rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Action-List**

### 2.70.5.3.1 Name

Specifies the name of a group of actions.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Action-List**

**Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Action-List**

**Possible values:**

Maximum 252 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

**Default:**

Blank

## 2.70.5.5 Station-List

You can group stations in this table. Define the actions previously under **Setup** > **IPv6** > **Firewall** > **Stations**.

**Note:** You can not delete a station in this list if the firewall is used in a forwarding or inbound rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations-List**

### 2.70.5.5.1 Name

Specifies the name of a group of stations.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations-List**

**Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.5.2 Beschreibung

Contains the list of stations that are grouped together under this group name.

Separate the individual entries with a comma.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations-List**

**Possible values:**

Maximum 252 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

**Default:**

Blank

## 2.70.5.6 Service-List

You can group services in this table. Define the services previously under **Setup** > **IPv6** > **Firewall** > **Services**.

**Note:** You can not delete a service in this list if the firewall is used in a forwarding or inbound rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Service-List**

### 2.70.5.6.1 Name

Specifies the name of a group of services.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Service-List**

**Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.6.2 Beschreibung

Contains the list of services that are grouped together under this group name.

Separate the individual entries with a comma.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Service-List**

**Possible values:**

Maximum 252 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**Default:**

Blank

## 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**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

### 2.70.5.7.1 Name

Specifies the name of the action.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.7.2 Limit

When this limit is exceeded, the firewall applies the filter rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Max. 10 characters from 0123456789

**Special values:**

0: The rule will come into force immediately.

**Default:**

0

### 2.70.5.7.3 Unit

Determines the unit for the limits.

**Telnet 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.

**Telnet 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. Possible values are:

- **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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Session

Station

Global

**Default:**

Session

### 2.70.5.7.6 Flags

Determines the properties of the limits of the action. Possible values are:

- **Reset**: If the limit is exceeded, the action resets the counter.
- **Shared:** All rules to which this limit applies use the same limit counter.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Reset

Shared

**Default:**

Blank

### 2.70.5.7.7 Action

Determines the action the firewall performs when the limit is reached.

The following options are possible:

- **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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Reject

Drop

Accept

**Default:**

.

### 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.

**Note:** Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

BE

EF

CS0 to CS7

AF11 to AF43

No

Value

**Special values:**

**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.

**Note:** Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Max. 2 characters from 1234567890

**Default:**

0

### 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**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

#### 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**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 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**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

#### 2.70.5.9.1 Name

Specifies the name of the station.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.9.2 Typ

Determines the station type.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**Possible values:**

Local network

Remote site

Prefix

Identifier

IP address

Named host

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**Possible values:**

Max. 16 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**Possible values:**

Maximum 64 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**Possible values:**

Max. 43 characters from ABCDEFabcdef0123456789:

**Default:**

Blank

### 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** > **Servicelist**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Services**

### 2.70.5.10.1 Name

Specifies the name of the service.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Services**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.10.2 Protocol

Specifies the protocol of the service.

**Telnet 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.

**Note:** Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Services**

**Possible values:**

Max. 64 characters from 0123456789,

**Default:**

Blank

#### 2.70.5.10.4 Src-Ports

Determines whether the specified ports are source ports.

**Note:** In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Stations**

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Protocols**

#### 2.70.5.11.1 Name

Specifies the name of the protocol.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Protocols**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

#### 2.70.5.11.2 Protocol

Specifies the protocol number.

**Note:** Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Protocols**

**Possible values:**

Max. 3 characters from 0123456789

**Default:**

Blank

### 2.70.5.12 Conditions

The firewall can perform the forwarding and inbound rule actions for the conditions listed in this table.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Conditions**

#### 2.70.5.12.1 Name

Specifies the name of the condition.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Conditions**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.12 Conditions

Specifies the conditions which must be met.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Conditions**

**Possible values:**

Not connected

Default route

Backup connection

VPN route

Transmitted

Received

**Default:**

Blank

#### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Conditions**

**Possible values:**

Physical

Logical

**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.

**Note:** Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

BE

EF

CS0 to CS7, CSx

AF11 to AF43, AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx

No

Value

**Special values:**

**CSx**: Extends the range to all class selectors.

**AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx**: Extends the range to include the corresponding assured forwarding classes (i.e. AF1x includes the categories AF11, AF12, AF13)

**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.

**Note:** Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Actions**

**Possible values:**

Max. 2 characters from 1234567890

**Default:**

0

### 2.70.5.13 Trigger actions

This table contains a list of the trigger actions, which the firewall actions can start.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

#### 2.70.5.13.1 Name

Specifies the name of the trigger action.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.13.2 Notifications

Determines whether and how a notification should be sent.

**Note:** If you want to receive e-mail notifications, you must enter an e-mail address in **Setup** > **IP-Router** > **Firewall** > **Admin-Email**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

**Possible values:**

SNMP

SYSLOG

E-mail

**Default:**

Blank

### 2.70.5.13.3 Disconnect

Determines whether the firewall disconnects the connection to the remote station if the filter condition is true.

**Telnet 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**.

#### Telnet path:

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

#### Possible values:

No

Yes

#### Default:

No

### 2.70.5.13.5 Lockout period

Specifies how many minutes the firewall blocks the source.

#### Telnet path:

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

#### Possible values:

Max. 8 characters from 0123456789

#### Special values:

0: Disables the lock because, in practice, the lockout period expires after 0 minutes.

#### Default:

0

### 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**.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

**Possible values:**

No

Yes

**Default:**

No

#### 2.70.5.13.7 Closing time

Determines, for how many seconds the firewall closes the destination.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Trigger-Actions**

**Possible values:**

Max. 8 characters from 0123456789

**Special values:**

0: Disables the lock because, in practice, the lockout period expires after 0 minutes.

**Default:**

0

### 2.70.5.14 ICMP-Services

This table contains a list of ICMP-service.

**Note:** Since ICMPv6 has central importance for numerous IPv6 features, basic ICMPv6 rules are already configured by default. You can not delete these rules.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **ICMP-Services**

### 2.70.5.14.1 Name

Specifies the name of the ICMP service.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **ICMP-Services**

**Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.14.2 Type

Specifies the type of the ICMP service.

**Note:** Lists with the official ICMP types and port codes are available in the Internet under *www.iana.org*.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **ICMP-Services**

**Possible values:**

Max. 3 characters from 0123456789

**Default:**

0

### 2.70.5.14.3 Code

Specifies the codes of the ICMP service.

**Note:** Lists with the official ICMP types and port codes are available in the Internet under *www.iana.org*.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **ICMP-Services**

**Possible values:**

Max. 3 characters from 0123456789

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

### 2.70.5.15.1 Name

Specifies the name of the inbound rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

**Default:**

Blank

### 2.70.5.15.2 Active

This option enables the inbound rule.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.70.5.15.3 Priority

This information determines the priority with which the firewall applies the rule. A higher value determines a higher priority.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Max. 4 characters from 1234567890

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQR-STUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqr-stuvwxyz`

**Default:**

ANYHOST

### 2.70.5.15.10 Comment

Enter a descriptive comment for this entry.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

Maximum 64 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

**Default:**

Blank

### 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.

**Telnet path:**

**Setup** > **IPv6** > **Firewall** > **Inbound-Rules**

**Possible values:**

0 to 65535

**Comment**

- 65535: The firewall rule is applied if the expected interface- or routing tag is 0.
- 1…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).

**Default:**

0

## 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.

**Telnet 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.

**Note:** The default value is set high enough to avoid triggering the IDS during normal operation.

**Telnet path:**

**Setup** > **IPv6** > **Firewall**

**Possible values:**

0 to 99999

**Default:**

300

## 2.70.6 LAN-Interfaces

This table contains the settings for the LAN interfaces.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces**

## 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.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

## 2.70.6.2 Interface-ID

Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Interface-ID**

**Possible values:**

All physically available interfaces on the device

**Default:**

LAN-1

## 2.70.6.3 VLAN-ID

Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.

**Note:** If you enter an invalid VLAN ID here, no communication will take place.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **VLAN-ID**

**Possible values:**

0 to 4096

Max. 4 numbers

**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.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 0 – 65535

**Default:**

0

## 2.70.6.5 Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

**Note:** If the device sends router advertisements from this interface, it does not generate any IPv6 addresses even with auto-configuration enabled.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Autoconf**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.6.6 Accept-RA

Enables or disables the processing of received router advertisement messages.

**Note:** With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Accept-RA**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.6.7 Interface-Status

Enables or disables this interface.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Interface-Status**

**Possible values:**

Up

Down

**Default:**

Up

## 2.70.6.8 Forwarding

Enables or disables the forwarding of data packets to other interfaces.

**Note:** With forwarding disabled, no router advertisements are transmitted from this interface.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Forwarding**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.6.9 MTU

Specify the applicable MTU for this interface.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **MTU**

**Possible values:**

Max. 4 numbers in the range 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** .

**Note:** If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Firewall**

**Possible values:**

Yes

No

**Default:**

No

## 2.70.6.11 Comment

Enter a descriptive comment for this entry.

**Note:** Entering a comment is optional.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **Comment**

**Possible values:**

Max. 64 characters

**Default:**

Blank

## 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.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces** > **DaD-Attempts**

**Possible values:**

0 to 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.

**Telnet path:**

**Setup** > **IPv6** > **LAN-Interfaces**

**Possible values:**

Max. 1 characters from `[0-9]`

**Default:**

3

## 2.70.7 WAN-Interfaces

This table contains the settings for the LAN interfaces.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces**

## 2.70.7.1 Interface-Name

Specify the name of the WAN remote peer here. Use the name as specified at the remote site.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Interface-Name**

**Possible values:**

Max. 16 characters

**Default:**

Blank

## 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.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Rtg-Tag**

**Possible values:**

Max. 5 characters in the range 0 – 65534

**Default:**

0

## 2.70.7.3 Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

**Note:** If the device sends router advertisements from this interface, it does not generate any addresses even with auto-configuration enabled.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Autoconf**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.7.4 Accept-RA

Enables or disables the processing of received router advertisement messages.

**Note:** With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Accept-RA**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.7.5 Interface-Status

Enables or disables this interface.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Interface-Status**

**Possible values:**

Up

Down

**Default:**

Up

## 2.70.7.6 Forwarding

Enables or disables the forwarding of data packets to other interfaces.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Forwarding**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.7.7 Firewall

Enables the firewall for this interface.

**Note:** If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Firewall**

**Possible values:**

Yes

No

**Default:**

Yes

## 2.70.7.8 Comment

Enter a descriptive comment for this entry.

**Note:** Entering a comment is optional.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **Comment**

**Possible values:**

Max. 64 characters

**Default:**

Blank

## 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.

**SNMP ID:**

2.70.7.9

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces** > **DaD-Attempts**

**Possible values:**

Max. 1 number

**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.

This option allows you to set the way the router performs the prefix delegation:

- DHCPv6: Prefix delegation is performed via DHCPv6
- Router advertisement: Prefix delegation is performed via router advertisement and the DHCPv6 client does not start.

**SNMP ID:**

2.70.7.10

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces**

**Possible values:**

DHCPv6

Router-Advertisement

**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.

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces**

**Possible values:**

Max. 1 characters from `[0-9]`

**Default:**

3

## 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.

**Telnet path:**

**Setup** > **IPv6** > **Operating**

**Possible values:**

Yes

No

**Default:**

No

## 2.70.11 Forwarding

If forwarding is turned off, the device transmits no data packets between IPv6 interfaces.

**Note:** Forwarding is essential if you wish to operate the device as a router.

**Telnet path:**

**Setup** > **IPv6** > **Forwarding**

**Possible values:**

Yes

No

**Default:**

Yes

### 2.70.12 Router

These are the router settings.

**Telnet path:**

**Setup** > **IPv6** > **Router**

## 2.70.12.1 Routing-Table

The table contains the entries to be used for routing packets with IPv6 addresses.

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Routing-Table**

#### 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

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Routing-Table** > **Prefix**

**Possible values:**

Max. 43 characters

**Default:**

Blank

#### 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.

**Note:** Routing tags are only necessary if used in combination with routing tags as set by firewall rules or as set at an interface.

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Routing-Table** > **Routing-Tag**

**Possible values:**

Max. 5 characters

**Default:**

Blank

### 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)

**Note:** The device stores the remote sites for IPv6 routing as (*WAN interfaces*).

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Routing-Table** > **Peer-or-IPv6**

**Possible values:**

Max. 56 characters

**Default:**

Blank

### 2.70.12.1.4 Comment

Enter a descriptive comment for this entry.

**Note:** Entering a comment is optional.

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Routing-Table** > **Comment**

**Possible values:**

Max. 64 characters

**Default:**

Blank

## 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.

**Telnet path:**

**Setup** > **IPv6** > **Router** > **Dest.-Cache-Timeout**

**Possible values:**

Max. 3 characters

**Default:**

30 seconds

## 2.70.13 ICMPv6

This menu contains the settings for ICMPv6.

**Telnet path:**

**Setup** > **IPv6**

## 2.70.13.1 Interface-Name

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".

**Telnet path:**

**Setup** > **IPv6** > **ICMPv6**

**Possible values:**

Selection from the list of LAN/WAN interfaces defined in the device; max. 16 characters

**Default:**

## 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.

**Telnet path:**

**Setup** > **IPv6** > **ICMPv6**

**Possible values:**

0 to 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).

**Telnet path:**

**Setup** > **IPv6** > **ICMPv6**

**Possible values:**

Activating the

Deactivating an

**Default:**

Activating the

### 2.70.14 RAS interface

In this directory, you specify the settings for RAS access via IPv6.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet 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**.

**Attention:** If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

**Telnet 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.

**Telnet 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.

**Telnet 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.

**Telnet path:**

**Setup** > **IPv6** > **RAS-Interface**

**Possible values:**

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

**Default:**

*empty*

# 2.80 Relays

Contains the settings for the relays. Relays are use to notify external systems about the devices status. The relays can be triggered via command line interface or by SNMP management software.

**Telnet path:** /Setup

## 2.80.1 Relay1

Close or open the relay using this switch. If the relay is closed, contacts will output a signal to external connected systems.

**Telnet path:** /Setup/Relays

**Possible values:**

- Yes: Relay is closed and signal is applied to the contacts.
- No: Relay is open and there is no signal applied to the contacts

**Default:** No

**Note:** After restart, reboot or firmware upload the relays are open, no signal is applied to the contacts.

## 2.80.2 Relay2

Close or open the relay using this switch. If the relay is closed, contacts will output a signal to external connected systems.

**Telnet path:** /Setup/Relays

**Possible values:**

- Yes: Relay is closed and signal is applied to the contacts.
- No: Relay is open and there is no signal applied to the contacts

**Default:** No

**Note:** After restart, reboot or firmware upload the relays are open, no signal is applied to the contacts.

# 3 Firmware

This menu contains the actions and settings options for managing the device firmware.

**Telnet path:** /Firmware

## 3.1 Version table

This table contains information about the firmware version and serial number of the device.

**Telnet path:** /Firmware/Version-Table

### 3.1.1 Ifc

The interface referred to by the entry.

**Telnet path:** /Firmware/Version-Table/Ifc

### 3.1.2 Module

Full description of the device type.

**Telnet path:** /Firmware/Version-Table/Module

### 3.1.3 Version

The firmware version currently active in the device, along with the release date.

**Telnet path:** /Firmware/Version-Table/Version

### 3.1.4 Serial number

The device serial number.

**Telnet path:** /Firmware/Version-Table/Serial-Number

# 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).

**Telnet path:** /Firmware/Table-Firmsafe

## 3.2.1 Position

Position in memory space of the current entry.

**Telnet path:** /Firmware/Table-Firmsafe/Position

## 3.2.2 Status

Status of the current entry.

Possible values:

- Inactive: This firmware is in a wait state and can be activated.
- Active: This firmware is currently in use in the device.
- Loader: This entry is not a firmware version but a loader with offering supporting functions.

**Telnet path:** /Firmware/Table-Firmsafe/Status

## 3.2.3 Version

Version descriptor of the firmware for the current entry.

**Telnet path:** /Firmware/Table-Firmsafe/Version

## 3.2.4 Date

Release date of the firmware for the current entry.

**Telnet path:** /Firmware/Table-Firmsafe/Date

### 3.2.5 Size

Size of the firmware for the current entry.

**Telnet path:** /Firmware/Table-Firmsafe/Size

### 3.2.6 Index

Index for the current entry.

**Telnet path:** /Firmware/Table-Firmsafe/Index

## 3.3 Firmsafe mode

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 firmsafe mode lets you decide which firmware is to be activated after the upload.

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.

- Manually: 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. Under WEBconfig you will find the firmsafe table under Firmware in the Expert configuration.

Default:

- Immediate

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.

**Telnet path:** /Firmware/Firmsafe-Mode

## 3.4 Timeout-Firmsafe

The time in seconds for testing new firmware.

Possible values:

- 0 to 99999 seconds.

Default:

- 300 seconds

**Telnet path:** /Firmware/Timeout-Firmsafe

## 3.7 Feature-Word

Displays the feature bits that provide information on the options activated in the device.

**Telnet path:** /Firmware/Feature-Word

# 4 Other

This menu contains additional functions from the HiLCOS menu tree.

**Telnet path:** Other

## 4.1 Manual dialing

This menu contains the actions for manual connection establishment.

**Telnet path:** /Other/Manual-Dialing

### 4.1.1 Connect

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.

**Telnet path:** /Other/Manual-Dialing/Connect

### 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.

**Telnet path:** /Other/Manual-Dialing/Disconnect

## 4.2 System-Boot

With this action you manually restart the device.

**Telnet path:**

**Other**

**Possible arguments:**

*none*

## 4.5 Cold boot

This action is used to reboot the device.

**Telnet path:** /Other/Cold-Boot

## 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.

**Telnet path:**

**Other** > **Flash-Restore**

# Further Support

### Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at
http://www.hirschmann.com

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at
https://hirschmann-support.belden.com

This site also includes a free of charge knowledge base and a software download section.

### Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

▶ Training offers you an introduction to the basics, product briefing and user training with certification.
You find the training courses on technology and products currently available at
https://www.belden.com/solutions/customer-innovation-center

▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against making any compromises in any case. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
https://www.belden.com/solutions/customer-innovation-center

HIRSCHMANN
A BELDEN BRAND

# Addendum

## HiLCOS Rel. 10.12

# 1 Configuration

## 1.1 Preventing password form fields in the browser from storing passwords

As of HiLCOS 10.12, it is possible to suppress the storage of passwords by your web browser for the WEBconfig login form.

Input dialogs on web pages allow web browsers to store any passwords that are entered. This makes things easier for a user accessing the page again in future. This web browser feature is a vulnerability that malicious software can exploit to read out the confidential form data.

To force the manual input of login passwords each time a page is accessed, open WEBconfig and navigate to **Setup** > **HTTP** > **Disable-Password-Autocompletion** and prevent the storage of passwords with the setting “Yes”.

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.21.22

**Telnet 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

# 1.2 Support of ChaCha20/Poly1305 for SSH access

As of version 10.12, HiLCOS additionally supports the following cipher algorithms for access via SSH:

- chacha20-poly1305
- aes128-gcm
- aes256-gcm

## Additions to the Setup menu

### Cipher-Algorithms

The cipher algorithms are used for encrypting and decrypting data. Select one or more of the available algorithms.

**SNMP ID:**

2.11.28.1

**Telnet 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

# 1.3 Enforcing password complexity for device passwords

## Additions to the Setup menu

### Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules.

**SNMP ID:**

2.11.93

**Telnet path:**

**Setup** > **Config**

**Possible values:**

**No**

Password rules enforcement is disabled.

**Yes**

Password rules enforcement is enabled.

**Default:**

Yes

# 1.4 Preventing the storage of passwords in WEBconfig

As of HiLCOS 10.12, you have the option to deactivate the auto-completion of password fields.

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.21.22

**Telnet 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

# 1.5 FirmSafe

## Additions to the Firmware menu

### 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.

**SNMP ID:**

3.8

**Telnet path:**

**Firmware**

**Possible values:**

**`do Switch-Firmware`**

Switch the firmware and restart the device

# 2 WLAN

## 2.1 Adaptive RF Optimization

### Additions to the Setup menu

#### 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.

**SNMP ID:**

2.23.20.23

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

**Ifc**

Shows the interface for the Adaptive RF Optimization.

**SNMP ID:**

2.23.20.23.1

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Operating**

Activates or deactivates Adaptive RF Optimization for this interface.

**SNMP ID:**

2.23.20.23.2

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Min-Client-Phy-Signal**

Setting for the minimum signal strength of clients.

**SNMP ID:**

2.23.20.23.3

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

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

**Default:**

15

**Min-Client-Tx-Packets**

Setting for the minimum number of packets sent to a client.

**SNMP ID:**

2.23.20.23.4

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

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

**Default:**

30

**Tx-Client-Retry-Ratio-Limit**

In this field you specify how quickly a packet is resent to a client.

**SNMP ID:**

2.23.20.23.5

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

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

**Default:**

70

**Noise-Limit**

Setting for the upper limit of acceptable noise on the channel.

**SNMP ID:**

2.23.20.23.6

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

Max. 6 characters from `[0-9]-`

**Default:**

-70

**Marked-Channel-Timeout**

When a channel is considered unusable it is marked/blocked for the time specified here.

**SNMP ID:**

2.23.20.23.7

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

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

**Default:**

20

**Trigger-Timespan**

The trigger timespan set here determines how long a limit is continuously exceeded before an action is triggered.

**SNMP ID:**

2.23.20.23.8

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

**Possible values:**

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

**Default:**

1

# 2.2 Airtime Fairness

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.9.6

**Telnet 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

# 2.3 Encrypted OKC via IAPP

## Additions to the Setup menu

### 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 Industrial HiVision.
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.

**SNMP ID:**

2.23.20.3.20

**Telnet 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.

# 2.4 Fast roaming

## Additions to the Setup menu

### 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 Industrial HiVision. 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.

**SNMP ID:**

2.23.20.3.20

**Telnet 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.

# 2.5 Adaptive transmission power

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.24

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

**Ifc**

The interface that this entry refers to.

**SNMP ID:**

2.23.20.24.1

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Redundancy-Settings**

**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.

**SNMP ID:**

2.23.20.24.2

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Redundancy-Settings**

**Possible values:**

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

**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.

**SNMP ID:**

2.23.20.24.3

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Redundancy-Settings**

**Possible values:**

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

# 2.6 Improved start-up conditions for WLAN RADIUS accounting

## Additions to the Setup menu

### Accounting-Start-Condition

Use this entry to specify when the DHCP server reports the beginning of a billing period to a RADIUS accounting server.

**SNMP ID:**

2.23.20.1.27

**Telnet 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

# 2.7 Selecting a RADIUS server profile for 802.1X authentication

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.3.21

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

# 2.8 Configurable data rates per WLAN module

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.25

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

**1M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.1

**Telnet 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

**2M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.2

**Telnet 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

**Ifc**

This entry shows which interface is being configured.

**SNMP ID:**

2.23.20.25.3

**Telnet path:**

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

**5.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.4

**Telnet 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

**11M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.6

**Telnet 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

**6M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.8

**Telnet 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

**9M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.9

**Telnet 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

**12M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.10

**Telnet 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

**18M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.11

**Telnet 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

**24M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.12

**Telnet 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

**36M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.13

**Telnet 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

**48M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.14

**Telnet 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

**54M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.15

**Telnet 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

**HT-1-6.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.28

**Telnet 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

**HT-1-13M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.29

**Telnet 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

**HT-1-19.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.30

**Telnet 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

**HT-1-26M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.31

**Telnet 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

**HT-1-39M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.32

**Telnet 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

**HT-1-52M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.33

**Telnet 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

**HT-1-58.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.34

**Telnet 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

**HT-1-65M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.35

**Telnet 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

**HT-2-13M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.36

**Telnet 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

**HT-2-26M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.37

**Telnet 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

**HT-2-39M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.38

**Telnet 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

**HT-2-52M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.39

**Telnet 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

**HT-2-78M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.40

**Telnet 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

**HT-2-104M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.41

**Telnet 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

**HT-2-117M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.142

**Telnet 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

**HT-2-130M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.43

**Telnet 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

**HT-3-19.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.44

**Telnet 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

**HT-3-39M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.45

**Telnet 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

**HT-3-58.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.46

**Telnet 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

**HT-3-78M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.47

**Telnet 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

**HT-3-117M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.48

**Telnet 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

**HT-3-156M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.49

**Telnet 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

**HT-3-175.5M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.50

**Telnet 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

**HT-3-195M**

Here you configure how the AP is to handle this data rate for this interface.

**SNMP ID:**

2.23.20.25.51

**Telnet 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

**VHT-1-Max-Tx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.105

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

**VHT-1-Max-Rx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.106

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

**VHT-2-Max-Tx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.115

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

**VHT-2-Max-Rx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.116

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

**VHT-3-Max-Tx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.125

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

**VHT-3-Max-Rx-MCS**

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

**SNMP ID:**

2.23.20.25.126

**Telnet path:**

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

**Possible values:**

**None**
**MCS7**
**MCS8**
**MCS9**

**Default:**

MCS9

## 2.9 Maximum length of the AP device name in the WLC config increased to 64 characters

As of HiLCOS 10.12, AP device names in the access point table can be specified using up to 64 characters.

## Additions to the Setup menu

### Name

Name of the AP in managed mode.

**SNMP ID:**

2.37.1.4.2

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

**Possible values:**

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

**Default:**

*empty*

# 2.10 Support for AiRISTA Flow Blink Mode (former Ekahau Blink Mode)

## Additions to the Setup menu

### Blink mode

This menu contains the settings for communications with the RTLS server (Ekahau RTLS Controller, ERC).

**SNMP ID:**

2.12.131

**Telnet path:**

**Setup** > **WLAN**

**Server address**

Contains the IP address or the DNS name of the RTLS server.

**SNMP ID:**

2.12.131.1

**Telnet path:**

**Setup** > **WLAN** > **Blink-Mode**

**Possible values:**

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

**Default:**

*empty*

**Server port**

Contains the UDP port number of the RTLS server.

**SNMP ID:**

2.12.131.2

**Telnet path:**

**Setup** > **WLAN** > **Blink-Mode**

**Possible values:**

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

**Default:**

8569

**Loopback address**

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

**SNMP ID:**

2.12.131.3

**Telnet path:**

**Setup** > **WLAN** > **Blink-Mode**

**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*

## Blink mode

In this table, you configure the blink mode for the physical WLAN interfaces.

**SNMP ID:**

2.23.20.26

**Telnet path:**

**Setup** > **Interfaces**

**Ifc**

Contains the name of the physical WLAN interface.

**SNMP ID:**

2.23.20.26.1

**Telnet path:**

**Setup** > **Interfaces** > **Blink-Mode**

**Possible values:**

**WLAN-1**
**WLAN-2**

**Operating**

Activates or deactivates the blink mode for this physical interface.

**SNMP ID:**

2.23.20.26.2

**Telnet path:**

**Setup** > **Interfaces** > **Blink-Mode**

**Possible values:**

**Yes**
**No**

**Default:**

No

**Network**

Here you select the logical WLAN interface that the device reports to the ERC.

**SNMP ID:**

2.23.20.26.3

**Telnet path:**

**Setup** > **Interfaces** > **Blink-Mode**

**Possible values:**

**List of the available logical WLAN interfaces 'WLAN-1' to 'WLAN-x'**

# 2.11 Managing WLAN sessions using RADIUS CoA

## Additions to the Setup menu

### Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176*.

**SNMP ID:**

2.25.19

**Telnet path:**

**Setup** > **RADIUS**

#### Operating

This entry enables or disables the dynamic authorization by RADIUS.

**SNMP ID:**

2.25.19.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

**No**
**Yes**

**Default:**

No

#### Port

This entry specifies the port on which CoA messages are accepted.

**SNMP ID:**

2.25.19.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

3799

**WAN access**

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

**SNMP ID:**

2.25.19.3

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Clients**

All of the CoA clients that send messages to the NAS are entered into this table.

**SNMP ID:**

2.25.19.4

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**HostName**

This entry contains the unique identifier of the client that sends messages to the NAS.

**SNMP ID:**

2.25.19.4.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Clients**

**Possible values:**

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

**Default:**

*empty*

### Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

**SNMP ID:**

2.25.19.4.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Clients**

**Possible values:**

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

**Default:**

*empty*

### Forward-Servers

To forward CoA messages, the forwarding servers are specified here.

**SNMP ID:**

2.25.19.5

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

### Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

**SNMP ID:**

2.25.19.5.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

**HostName**

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

**SNMP ID:**

2.25.19.5.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

**Port**

This entry contains the port for communications with the forwarding server.

**SNMP ID:**

2.25.19.5.3

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

0

**Secret**

This entry specifies the secret required to access the forwarding server.

**SNMP ID:**

2.25.19.5.4

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

### 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.

**SNMP ID:**

2.25.19.5.5

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

### Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

**SNMP ID:**

2.25.19.6

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

*empty*

### Empty realm

This realm is used when the specified username does not contain a realm.

**SNMP ID:**

2.25.19.7

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

*empty*

**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 HiLCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

**SNMP ID:**

2.25.19.8

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

### Dyn-Auth

This entry enables or disables dynamic authorization by RADIUS CoA on the corresponding interface.

**SNMP ID:**

2.23.20.1.28

**Telnet path:**

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

**Possible values:**

**No**
**Yes**

**Default:**

No

# 2.12 Selectively allowing inter-station traffic for clients on the same VLAN

## Additions to the Setup menu

### VLAN no interstation traffic

This table contains combinations of SSIDs and VLANs for which data exchange between clients should be prohibited.

**SNMP ID:**

2.12.71

**Telnet path:**

**Setup** > **WLAN**

**Network**

From the list of available SSIDs, select the network for which data exchange between clients should be prohibited.

**SNMP ID:**

2.12.71.1

**Telnet path:**

**Setup** > **WLAN** > **VLAN-No-Interstation-Traffic**

**VLAN-ID**

Here you specify the VLAN ID for which data exchange between clients should be prohibited.

**SNMP ID:**

2.12.71.2

**Telnet path:**

**Setup** > **WLAN** > **VLAN-No-Interstation-Traffic**

**Possible values:**

1 … 4094

**Default:**

0

# 2.13 Starting an environment scan at a configurable time

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.27

**Telnet path:**

**Setup** > **Interfaces** > **WLAN**

**Ifc**

This table contains the available WLAN interfaces.

**SNMP ID:**

2.23.20.27.1

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Environment-Scan**

**Possible values:**

**1**

WLAN-1

**2**

WLAN-2

**Yes**

Enables/disables the environment scan.

**SNMP ID:**

2.23.20.27.2

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Environment-Scan**

**Possible values:**

**0**

Not active

**1**

Active

**Default:**

0

**Hours**

Set the hours value for the time of the environment scan here.

**SNMP ID:**

2.23.20.27.6

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Environment-Scan**

**Possible values:**

0 … 23

**Default:**

3

**Minutes**

Set the minutes value for the time of the environment scan here.

**SNMP ID:**

2.23.20.27.7

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Environment-Scan**

**Possible values:**

0 … 59

**Default:**

0

**Frequency band**

Here you set the radio band for which your WLAN module performs an environment scan.

**SNMP ID:**

2.23.20.27.8

**Telnet 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

**Subbands-5GHz**

Here you configure the subbands of your 5-GHz frequency band.

**SNMP ID:**

2.23.20.27.9

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Environment-Scan**

**Possible values:**

**1+2+3**
**1+2**
**1+3**
**2+3**
**1**
**2**
**3**

**Default:**

1+2+3

**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.

**SNMP ID:**

2.23.20.27.10

**Telnet 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.

# 2.14 Converting data streams from multicast into unicast

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.2.25

**Telnet 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

# 3 WLAN Management

## 3.1 Multiple configurable AutoWDS profiles

As of HiLCOS 10.12 WLCs are able to manage multiple AutoWDS profiles.

### Additions to the Setup menu

#### 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).

**SNMP ID:**

2.37.1.15

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

**Name**

Name of the AutoWDS profile which you reference from other tables.

The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.

**SNMP ID:**

2.37.1.15.1

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

**Possible values:**

Max. 15 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

**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.

**SNMP ID:**

2.37.1.15.2

**Telnet 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*

**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.

**SNMP ID:**

2.37.1.15.3

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

**Possible values:**

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

**Default:**

AutoWDS-Rollout

## AutoWDS-Topology

Name of the AutoWDS profile for which this manual P2P configuration applies.

**SNMP ID:**

2.37.1.16.1

**Telnet 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*

# 3.2 WLC script rollout for certain versions of HiLCOS

As of HiLCOS 10.12, you have the option of specifying WLC-controlled script rollouts for certain versions of HiLCOS. This allows different versions of HiLCOS with their differing configurations to integrate into a common WLAN installation.

## Additions to the Setup menu

### 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. 10.12

**SNMP ID:**

2.37.27.16.3

**Telnet path:**

**Setup** > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

**Possible values:**

Max. 6 characters from `[0-9].`

**Default:**

*empty*

# 3.3 RADIUS

## Additions to the Setup menu

### Availability monitoring

In this directory you configure the availability monitoring.

Monitoring is performed by sending status server requests or access requests.

**SNMP ID:**

2.25.21

**Telnet path:**

**Setup** > **RADIUS**

### Profiles

Here you create monitoring profiles for the availability of RADIUS servers.

**SNMP ID:**

2.25.21.1

**Telnet path:**

**Setup** > **RADIUS** > **Supervision-Servers**

## Name

Enter the name of the availability monitoring profile here.

**SNMP ID:**

2.25.21.1.1

**Telnet path:**

**Setup** > **RADIUS** > **Supervision-Servers** > **Profiles**

**Possible values:**

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

**Default:**

DEFAULT

## Type

Here, you specify whether status server or access requests are sent to the RADIUS server for the purpose of availability monitoring.

**SNMP ID:**

2.25.21.1.2

**Telnet path:**

**Setup** > **RADIUS** > **Supervision-Servers** > **Profiles**

**Possible values:**

**Access request**
**Status server**

**Default:**

Access request

## 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.

**SNMP ID:**

2.25.21.1.3

**Telnet path:**

**Setup** > **RADIUS** > **Supervision-Servers** > **Profiles**

**Possible values:**

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

**Default:**

*empty*

### Request interval

Here you define the interval in seconds used by the RADIUS server to check the availability.

**SNMP ID:**

2.25.21.1.4

**Telnet path:**

**Setup** > **RADIUS** > **Supervision-Servers** > **Profiles**

**Possible values:**

`[0-9]`

**Default:**

60

# 3.4 Coordinated channel selection for Wireless ePaper

## Additions to the Setup menu

### Channel coordination

Prevents collisions on ePaper channels due to APs within range of each other.

**SNMP ID:**

2.88.4

**Telnet path:**

**Setup** > **Wireless-ePaper**

**Operating**

The coordinated channel selection is activated or deactivated here.

**SNMP ID:**

2.88.4.1

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

**0**

No

**1**

Yes

**Default:**

1

**Network**

Here you specify the network that the access points are to use to communicate with each other.

**SNMP ID:**

2.88.4.2

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

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

**Announce address**

Set the announce address here.

**SNMP ID:**

2.88.4.3

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

39 characters from the following character set: `[0-9 A-F a-f :.]`

**Announce port**

Set the announce port here.

**SNMP ID:**

2.88.4.4

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

5 characters from the following character set: `[0-9]`

**Announce interval**

Set the announce interval here.

**SNMP ID:**

2.88.4.5

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

10 characters from the following character set: `[0-9]`

**Announce timeout factor**

Set the announce timeout factor here.

**SNMP ID:**

2.88.4.6

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

5 characters from the following character set: `[0-9]`

**Announce timeout interval**

Set the announce timeout interval here.

**SNMP ID:**

2.88.4.7

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

10 characters from the following character set: `[0-9]`

**Announce master backoff interval**

Set the announce master backoff interval here.

**SNMP ID:**

2.88.4.8

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

3 characters from the following character set: `[0-9]`

**Coordination port**

Set the coordination port here.

**SNMP ID:**

2.88.4.9

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

5 characters from the following character set: `[0-9]`

#### Coordination keep-alive interval

Here you set the coordination keep-alive interval.

**SNMP ID:**

2.88.4.10

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

10 characters from the following character set: `[0-9]`

#### Coordination reconnect interval

Here you set the coordination reconnect interval.

**SNMP ID:**

2.88.4.11

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

10 characters from the following character set: `[0-9]`

#### Assignment switch threshold

Here you set the assignment switch threshold.

**SNMP ID:**

2.88.4.12

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

3 characters from the following character set: `[0-9]`

**Distance weighting**

Here you set the weighting of WLAN distance.

A higher value means a better weighting.

**SNMP ID:**

2.88.4.13

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

0 … 255

**Channel weighting**

Here you set the weighting of a preferred channel.

A higher value means a better weighting.

**SNMP ID:**

2.88.4.14

**Telnet path:**

**Setup** > **Wireless-ePaper** > **Channel-Coordination**

**Possible values:**

0 … 255

# 3.5 Backup connections for dual-SIM services

**Additions to the Setup menu**

**Fallback minutes**

Specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

**SNMP ID:**

2.2.24.4

**Telnet path:**

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

**Possible values:**

Max. 4 characters from `0123456789`

**Default:**

0

**Special values:**

**0**

The backup connection remains active permanently.

# 4 Public Spot

## 4.1 Creating Public Spot users on a remote Public Spot gateway

### Additions to the Setup menu

#### 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.

**SNMP ID:**

2.24.41.5

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules**

**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.

**SNMP ID:**

2.24.41.5.1

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

**Possible values:**

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

**Default:**

*empty*

**Name**

Use this entry to specify which administrator account is used for creating user accounts on the remote Public Spot gateway.

**SNMP ID:**

2.24.41.5.2

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

**Possible values:**

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

**Default:**

*empty*

**Password**

Use this entry to enter the password for the administrator account specified above.

**SNMP ID:**

2.24.41.5.3

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

**Possible values:**

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

**Default:**

*empty*

# 4.2 Hiding fields in the setup wizard "Manage Public Spot Account"

## Additions to the Setup menu

### Show expiry type

This entry gives you the option to hide the "Expiry type" column in the Setup Wizard.

**SNMP ID:**

2.24.44.12

**Telnet 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

### Show abs. expiry

This entry gives you the option to hide the "Absolute expiry" column in the Setup Wizard.

**SNMP ID:**

2.24.44.13

**Telnet 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

**Show rel. expiry**

This entry gives you the option to hide the "Relative expiry" column in the Setup Wizard.

**SNMP ID:**

2.24.44.14

**Telnet 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

**Show time budget**

This entry gives you the option to hide the "Time budget" column in the Setup Wizard.

**SNMP ID:**

2.24.44.15

**Telnet 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

**Show volume budget**

This entry gives you the option to hide the "Volume budget MByte" column in the Setup Wizard.

**SNMP ID:**

2.24.44.16

**Telnet 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

**Show case sensitive**

This entry gives you the option to hide the "Case sensitive" column in the Setup Wizard.

**SNMP ID:**

2.24.44.17

**Telnet 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

**Show active**

This entry gives you the option to hide the "Show active" column in the Setup Wizard.

**SNMP ID:**

2.24.44.18

**Telnet 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

**Show TX limit**

This entry gives you the option to hide the "TX limit" (max. transmission bandwidth) column in the Setup Wizard.

**SNMP ID:**

2.24.44.19

**Telnet 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

**Show RX limit**

This entry gives you the option to hide the "RX limit" (max. receiving bandwidth) column in the Setup Wizard.

**SNMP ID:**

2.24.44.20

**Telnet 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

**Show calling station**

This entry gives you the option to hide the "Show calling station" column in the Setup Wizard.

**SNMP ID:**

2.24.44.21

**Telnet 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

**Show called station**

This entry gives you the option to hide the "Show called station" column in the Setup Wizard.

**SNMP ID:**

2.24.44.22

**Telnet 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

**Show online time**

This entry gives you the option to hide the "Online time" column in the Setup Wizard.

**SNMP ID:**

2.24.44.23

**Telnet 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

**Show traffic**

This entry gives you the option to hide the "Traffic (Rx / Tx Kbyte)" column in the Setup Wizard.

**SNMP ID:**

2.24.44.24

**Telnet 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

**Show status column**

This entry gives you the option to hide the "Status" column in the Setup Wizard.

**SNMP ID:**

2.24.44.25

**Telnet 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

**Show MAC address**

This entry gives you the option to hide the "MAC address" column in the Setup Wizard.

**SNMP ID:**

2.24.44.26

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Manage-User-Wizard**

**Possible values:**

**Yes**
The Setup Wizard shows the "MAC address" column.

# 4.3 Redirect for HTTPS connections switchable

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.24.51

**Telnet 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

# 4.4 Logging DNS requests and responses to external SYSLOG servers

## Additions to the Setup menu

**SNMP ID:** **Syslog**

2.17.20 Use this directory to configure the SYSLOG logging of DNS requests.

**Telnet path:**

**Setup** > **DNS**

#### 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`)

**SNMP ID:**

2.17.20.1

**Telnet 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

#### 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.

**SNMP ID:**

2.17.20.2

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

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

**Log source**

Contains the log source as displayed in the SYSLOG messages.

**SNMP ID:**

2.17.20.3

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

**System**
**Login**
**System time**
**Console login**
**Connections**
**Accounting**
**Administration**
**Router**

**Default:**

Router

**Log level**

Contains the priority that is shown in the SYSLOG messages.

**SNMP ID:**

2.17.20.4

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

**Emergency**
**Alert**
**Critical**
**Error**
**Warning**
**Notice**
**Info**
**Debug**

**Default:**

Notice

**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.

**SNMP ID:**

2.17.20.5

**Telnet 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**

## Facility

The mapping of sources to specific facilities.

**SNMP ID:**

2.22.3.2

**Telnet 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**

## 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.

**SNMP ID:**

2.22.2.7

**Telnet path:**

**Setup** > **SYSLOG** > **SYSLOG table**

**Possible values:**

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

# 4.5 Protection against brute force attacks

## Additions to the Setup menu

### Brute force protection

This menu contains the settings for the brute-force protection used by the Public Spot.

**SNMP ID:**

2.24.49

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Max. login tries**

Specify how many unsuccessful attempts are permitted before the login block takes effect.

**SNMP ID:**

2.24.49.1

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Brute-Force-Protection**

**Possible values:**

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

**Default:**

10

**Blocking time in minutes**

Specify how long the login block of the brute-force protection applies.

**SNMP ID:**

2.24.49.2

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Brute-Force-Protection**

**Possible values:**

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

**Default:**

60

**Unblocking check in seconds**

Specify the interval after which the AP checks for the expiry of a login block for a MAC address.

**SNMP ID:**

2.24.49.3

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Brute-Force-Protection**

**Possible values:**

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

**Default:**

60

**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`.

**SNMP ID:**

2.24.49.4

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Brute-Force-Protection**

# 4.6 Requesting the user e-mail address upon "login via agreement"

## Additions to the Setup menu

### Require e-mail

This entry allows you to specify whether the e-mail address of the user should be requested.

**SNMP ID:**

2.24.41.4.4

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

**Possible values:**

**No**
**Yes**

**Default:**

No

### 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.

**SNMP ID:**

2.24.41.4.7

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

**Possible values:**

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

# 4.7 Configuring the headline of the Public Spot login page

## Additions to the Setup menu

### 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).

**SNMP ID:**

2.24.61

**Telnet path:**

**Setup** > **Public-Spot-Module**

**Language**

This entry displays the language selected for the login title.

**SNMP ID:**

2.24.61.1

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Login-Instructions**

**Contents**

Enter the login title for your Public Spot here.

**SNMP ID:**

2.24.61.1

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Login-Instructions**

**Possible values:**

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

**Default:**

*empty*

# 4.8 Confirmation of the terms of use on the PMS-login page

## Additions to the Setup menu

### User-Must-Accept-GTC

With this setting you enable or disable the confirmation of the terms of use on the PMS-login page.

**SNMP ID:**

2.64.11.14

**Telnet 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

# 4.9 Tx and Rx bandwidths configurable for rates in the PMS module

## Additions to the Setup menu

### Name

Use this entry to specify a name for this rate.

**SNMP ID:**

2.64.15.4

**Telnet path:**

**Setup** > **PMS-Interface** > **Rate**

**Possible values:**

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

## Tx bandwidth

Use this entry to restrict the transmit (Tx) bandwidth.

**SNMP ID:**

2.64.15.5

**Telnet 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.

## Rx bandwidth

Use this entry to restrict the receive (Rx) bandwidth.

**SNMP ID:**

2.64.15.6

**Telnet 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.

# 4.10 Support for RADIUS CoA

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.24.55

**Telnet 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

# 4.11 Independent user authentication (Smart Ticket)

## Additions to the Setup menu

### Restricting the allowed country codes when using SmartTicket via SMS

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.

**SNMP ID:**

2.24.41.2.26

**Telnet path:**

**Setup** > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

**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.

**SNMP ID:**

2.24.41.2.26.1

**Telnet 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

# 5 VPN

## 5.1 IKEv2 support

### Additions to the Setup menu

#### IKEv2

In this directory you configure the IKEv2 parameters.

**SNMP ID:**

2.19.36

**Telnet path:**

**Setup** > **VPN**

**remote sites**

In this table, you configure the IKEv2 connections to VPN partners.

The console command `show vpn` shows whether the connection is successful.

**SNMP ID:**

2.19.36.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Peer**

Contains the name of the connection to the remote station.

Subsequently, this name appears in the routing table.

**SNMP ID:**

2.19.36.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

DEFAULT

**Active**

Specifies whether the VPN peer is enabled.

**SNMP ID:**

2.19.36.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

**Yes**

The VPN connection is enabled.

**No**

The VPN connection is disabled.

**Default:**

Yes

**SH time**

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

**SNMP ID:**

2.19.36.1.3

**Telnet 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.

**Remote gateway**

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

**SNMP ID:**

2.19.36.1.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

Max. 40 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

**Rtg-Tag**

Contains the routing tag for this VPN connection.

**SNMP ID:**

2.19.36.1.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

0

### Encryption

Specifies the encryption method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Encryption**.

**SNMP ID:**

2.19.36.1.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

DEFAULT

### Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

**SNMP ID:**

2.19.36.1.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

### General

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **General**.

**SNMP ID:**

2.19.36.1.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

DEFAULT

### Lifetimes

Specifies the lifetimes of the key used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Lifetimes**.

**SNMP ID:**

2.19.36.1.9

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

DEFAULT

### IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

**SNMP ID:**

2.19.36.1.10

**Telnet 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

**Rule creation**

Specifies how VPN rules are created.

**SNMP ID:**

2.19.36.1.11

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

**Auto**
The device creates the VPN rules automatically.

**Manual**
The device uses manually created rules.

**Default:**

Auto

**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**.

**SNMP ID:**

2.19.36.1.12

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

**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**.

**SNMP ID:**

2.19.36.1.13

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

**Comment**

Enter a comment about this entry.

**SNMP ID:**

2.19.36.1.17

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

**IPv4-CFG-Pool**

Use this entry to specify an IPv4 address pool for the IKEv2 peer.

**SNMP ID:**

2.19.36.1.18

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

**IPv6-CFG-Pool**

Use this entry to specify an IPv6 address pool for the IKEv2 peer.

**SNMP ID:**

2.19.36.1.19

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Encryption**

Use this table to configure the parameters for the IKEv2 encryption.

**SNMP ID:**

2.19.36.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Name**

Contains the name of this configuration.

**SNMP ID:**

2.19.36.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

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

**Default:**

DEFAULT

**DH-Groups**

Contains the selection of Diffie-Hellman groups.

**SNMP ID:**

2.19.36.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**DH16**
**DH15**
**DH14**
**DH5**
**DH2**

**Default:**

DH14

**PFS**

Specifies whether perfect forward secrecy (PFS) is enabled.

**SNMP ID:**

2.19.36.2.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**Yes**
**No**

**Default:**

Yes

**IKE-SA cipher list**

Specifies which encryption algorithms are enabled.

**SNMP ID:**

2.19.36.2.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**AES-CBC-256**
**AES-CBC-192**
**AES-CBC-128**
**3DES**

**Default:**

AES-CBC-256

**IKE-SA-Integ-Alg-List**

Specifies which hash algorithms are enabled.

**SNMP ID:**

2.19.36.2.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**SHA-512**
**SHA-384**
**SHA-256**
**SHA1**
**MD5**

**Default:**

SHA-256

SHA1

**Child-SA-Cipher-List**

Specifies which encryption algorithms are enabled in the Child-SA.

**SNMP ID:**

2.19.36.2.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**AES-CBC-256**
**AES-CBC-192**
**AES-CBC-128**
**3DES**

**Default:**

AES-CBC-256

**Child-SA-Integ-Alg-List**

Specifies which hash algorithms are enabled in the Child-SA.

**SNMP ID:**

2.19.36.2.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**SHA-512**
**SHA-384**
**SHA-256**
**SHA1**
**MD5**

**Default:**

SHA-256

SHA1

**Auth**

Use this menu to configure the parameters for the IKEv2 authentication.

**SNMP ID:**

2.19.36.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Parameter**

Use this table to configure the local and a corresponding remote identity for the IKEv2 authentication.

**SNMP ID:**

2.19.36.3.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth**

## Name

Contains the name of this entry.

**SNMP ID:**

2.19.36.3.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

DEFAULT

## Local-Auth

Sets the authentication method for the local identity.

**SNMP ID:**

2.19.36.3.1.2

**Telnet 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*.

**Default:**

PSK

### Local-ID-Type

Displays the ID type of the local identity. The device interprets the entry under **Local-ID** accordingly.

**SNMP ID:**

2.19.36.3.1.3

**Telnet 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

### Local-ID

Contains the local identity. The significance of this entry depends on the setting under **Local-ID-Type**.

**SNMP ID:**

2.19.36.3.1.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

### Local-Password

Contains the password of the local identity.

**SNMP ID:**

2.19.36.3.1.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

## Remote-Auth

Sets the authentication method for the remote identity.

**SNMP ID:**

2.19.36.3.1.6

**Telnet 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*.

**Default:**

PSK

## Remote-ID-Type

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

**SNMP ID:**

2.19.36.3.1.7

**Telnet 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

## Remote-ID

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

**SNMP ID:**

2.19.36.3.1.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

## Remote-Password

Contains the password of the remote identity.

**SNMP ID:**

2.19.36.3.1.9

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

### 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**.

**SNMP ID:**

2.19.36.3.1.11

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

### Remote-Cert-ID-Check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

**SNMP ID:**

2.19.36.3.1.12

**Telnet 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

### Local-Dig-Sig-Profile

Contains the profile name of the local digital signature profile being used.

**SNMP ID:**

2.19.36.3.1.13

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

## Remote-Dig-Sig-Profile

Contains the profile name of the remote digital signature profile.

**SNMP ID:**

2.19.36.3.1.14

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

## 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.

**SNMP ID:**

2.19.36.3.1.15

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

**Yes**
**No**

**Default:**

No

**General**

Use this table to configure the general IKEv2 parameters.

**SNMP ID:**

2.19.36.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Name**

Contains the name of this entry.

**SNMP ID:**

2.19.36.4.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

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

**Default:**

DEFAULT

**DPD-Inact-Timeout**

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

**SNMP ID:**

2.19.36.4.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

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

**Default:**

30

**SSL-Encaps.**

Specifies whether the connection uses IKEv2 over HTTPS.

**SNMP ID:**

2.19.36.4.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

**Yes**
**No**

**Default:**

No

**IPCOMP**

Specifies whether the devices transmit compressed IKEv2 data packets.

**SNMP ID:**

2.19.36.4.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

**Yes**
**No**

**Default:**

No

**Encaps-Mode**

Specifies the mode of transmission.

**SNMP ID:**

2.19.36.4.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

**Tunnel**

**Default:**

Tunnel

**Lifetimes**

Use this table to configure the lifetimes of the IKEv2 keys.

**SNMP ID:**

2.19.36.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Name**

Contains the name of this entry.

**SNMP ID:**

2.19.36.5.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Lifetimes**

**Possible values:**

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

**Default:**

DEFAULT

**IKE-SA-Sec**

Contains the time in seconds until the IKE SA key is renewed.

**SNMP ID:**

2.19.36.5.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Lifetimes**

**Possible values:**

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

**Default:**

108000

**Special values:**

**0**

No key renewal.

**IKE-SA-KB**

Contains the data volume in kilobytes until the IKE SA key is renewed.

**SNMP ID:**

2.19.36.5.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Lifetimes**

**Possible values:**

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

**Default:**

0

**Special values:**

**0**

No key renewal.

**Child-SA-Sec**

Contains the time in seconds until the CHILD SA key is renewed.

**SNMP ID:**

2.19.36.5.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Lifetimes**

**Possible values:**

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

**Default:**

28800

**Special values:**

**0**

No key renewal.

**Child-SA-KB**

Contains the data volume in kilobytes until the CHILD SA key is renewed.

**SNMP ID:**

2.19.36.5.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Lifetimes**

**Possible values:**

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

**Default:**

2000000

**Special values:**

**0**

No key renewal.

**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.

**SNMP ID:**

2.19.36.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**IPv4**

In this table, you configure the IPv4 addresses of the address pool for the IKEv2-CFG mode “Server”.

**SNMP ID:**

2.19.36.7.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG**

## Name

Contains the name of the IPv4 address pool.

**SNMP ID:**

2.19.36.7.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

**Possible values:**

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

## Start-Address-Pool

Here you enter the first IPv4 address of the pool of addresses that you want to provide to dial-in clients.

**SNMP ID:**

2.19.36.7.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

**Possible values:**

Max. 15 characters from `[0-9]./`

**Default:**

*empty*

## End-Address-Pool

Here you enter the last IPv4 address of the pool of addresses that you want to provide to dial-in clients.

**SNMP ID:**

2.19.36.7.1.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

**Possible values:**

Max. 15 characters from `[0-9]./`

**Default:**

*empty*

## Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

**SNMP ID:**

2.19.36.7.1.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

**Possible values:**

Max. 15 characters from `[0-9].`

**Default:**

0.0.0.0

### 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.

**SNMP ID:**

2.19.36.7.1.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

**Possible values:**

Max. 15 characters from `[0-9].`

**Default:**

*empty*

## IPv6

In this table, you configure the IPv6 addresses of the address pool for the IKEv2-CFG mode “Server”.

**SNMP ID:**

2.19.36.7.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG**

### Name

Contains the name of the IPv6 address pool.

**SNMP ID:**

2.19.36.7.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

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

## Start-Address-Pool

Here you enter the first IPv6 address of the pool of addresses that you want to provide to dial-in clients.

**SNMP ID:**

2.19.36.7.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

## End-Address-Pool

Here you enter the last IPv6 address of the pool of addresses that you want to provide to dial-in clients.

**SNMP ID:**

2.19.36.7.2.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

## Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

**SNMP ID:**

2.19.36.7.2.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

### 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.

**SNMP ID:**

2.19.36.7.2.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

# 5.2 IKEv2 fragmentation support

## Additions to the Setup menu

### MTU

This entry contains the maximum transmission unit (MTU) for IKEv2.

**SNMP ID:**

2.19.36.8

**Telnet 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.

# 5.3 RADIUS support for IKEv2

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.19.36.1.15

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

### 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.

**SNMP ID:**

2.19.36.1.16

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

### RADIUS

This menu contains the RADIUS configuration for IKEv2.

**SNMP ID:**

2.19.36.9

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Authorization**

This menu contains the configuration for the RADIUS authorization via IKEv2.

**SNMP ID:**

2.19.36.9.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS**

**Servers**

This table contains the server configuration for the RADIUS authorization under IKEv2.

**SNMP ID:**

2.19.36.9.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

## Name

Specify an identifier for this entry.

**SNMP ID:**

2.19.36.9.1.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

### Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

**SNMP ID:**

2.19.36.9.1.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

### Port

Specify the UDP port of the RADIUS server.

**SNMP ID:**

2.19.36.9.1.1.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

1812

### Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

**SNMP ID:**

2.19.36.9.1.1.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

## Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

**SNMP ID:**

2.19.36.9.1.1.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

**RADIUS**
**RADSEC**

**Default:**

RADIUS

## Loopback address

This entry contains the loopback address of the Hirschmann gateway that sent the request to the RADIUS server.

**SNMP ID:**

2.19.36.9.1.1.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

## Attribute-Values

HiLCOS 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`.

**SNMP ID:**

2.19.36.9.1.1.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

## Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

**SNMP ID:**

2.19.36.9.1.1.9

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

**Possible values:**

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

**Default:**

*empty*

### 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 Hirschmann 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.

**SNMP ID:**

2.19.36.9.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

**Possible values:**

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

**Default:**

*empty*

### Accounting

This menu contains the configuration for the RADIUS accounting via IKEv2.

**SNMP ID:**

2.19.36.9.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS**

### Server

This table contains the server configuration for the RADIUS accounting under IKEv2.

**SNMP ID:**

2.19.36.9.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

### Name

Specify an identifier for this entry.

**SNMP ID:**

2.19.36.9.2.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

### Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

**SNMP ID:**

2.19.36.9.2.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

### Port

Specify the UDP port of the RADIUS server.

**SNMP ID:**

2.19.36.9.2.1.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

1813

### Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

**SNMP ID:**

2.19.36.9.2.1.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

### Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

**SNMP ID:**

2.19.36.9.2.1.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

**RADIUS**
**RADSEC**

**Default:**

RADIUS

### Loopback address

This entry contains the loopback address of the Hirschmann gateway that sent the request to the RADIUS server.

**SNMP ID:**

2.19.36.9.2.1.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

## Attribute-Values

HiLCOS 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`.

**SNMP ID:**

2.19.36.9.2.1.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

## Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

**SNMP ID:**

2.19.36.9.2.1.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.19.36.9.2.2

**Telnet 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.

## 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.

**SNMP ID:**

2.19.36.10

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Possible values:**

**No**

No routes are generated for RAS SAs.

**Yes**

Routes are generated for RAS SAs.

**Default:**

Yes

## Extended parameters

This table contains extended parameters for IKEv2 remote stations.

**SNMP ID:**

2.19.36.11

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Name**

Name of the remote device.

**SNMP ID:**

2.19.36.11.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Extended-Parameters**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.19.36.11.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Extended-Parameters**

**Possible values:**

**Yes**
**No**

**Default:**

No

# 5.4 IKEv2 routing support

## Additions to the Setup menu

### 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**.

**SNMP ID:**

2.19.36.1.14

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

*empty*

## 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.

**SNMP ID:**

2.19.36.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

### IPv4

Use this table to configure the IPv4 tables for the IKEv2 routing.

**SNMP ID:**

2.19.36.6.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing**

#### Name

Contains the name of this entry.

**SNMP ID:**

2.19.36.6.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv4**

**Possible values:**

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

**Default:**

DEFAULT

#### Networks

Contains the comma-separated list of IPv4 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

**SNMP ID:**

2.19.36.6.1.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv4**

**Possible values:**

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

**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. Hirschmann routers generate the necessary routes automatically.

**SNMP ID:**

2.19.36.6.1.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv4**

**Possible values:**

**No**

The IPv4 address is not sent

**Yes**

The IPv4 address will be sent

**Default:**

Yes

**IPv6**

Use this table to configure the IPv6 tables for the IKEv2 routing.

**SNMP ID:**

2.19.36.6.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing**

**Name**

Contains the name of this entry.

**SNMP ID:**

2.19.36.6.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv6**

**Possible values:**

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

**Default:**

DEFAULT

**Networks**

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

**SNMP ID:**

2.19.36.6.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv6**

**Possible values:**

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

**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. Hirschmann routers generate the necessary routes automatically.

**SNMP ID:**

2.19.36.6.2.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Routing** > **IPv6**

**Possible values:**

**No**
The IPv6 address is not sent

**Yes**
The IPv6 address will be sent

**Default:**

Yes

# 5.5 "Match Remote Identity" for IKEv2

## Additions to the Setup menu

### Addit.-Remote-ID-List

Contains additional remote identities as specified in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**.

**SNMP ID:**

2.19.36.3.1.10

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**

**Possible values:**

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

**Default:**

*empty*

## Addit.-Remote-ID-List

Use this table to configure lists of additional remote identities.

**SNMP ID:**

2.19.36.3.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth**

**Name**

Sets the name of the ID list.

**SNMP ID:**

2.19.36.3.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.19.36.3.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

**Possible values:**

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

**Default:**

*empty*

## Addit.-Remote-IDs

Use this table to configure additional remote identities.

**SNMP ID:**

2.19.36.3.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth**

### Name

Contains the name of this remote identity.

**SNMP ID:**

2.19.36.3.3.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

**Possible values:**

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

**Default:**

*empty*

### Remote-Auth

Sets the authentication method for the remote identity.

**SNMP ID:**

2.19.36.3.3.2

**Telnet 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*.

**Default:**

PSK

**Remote-ID-Type**

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

**SNMP ID:**

2.19.36.3.3.3

**Telnet 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

**Remote-ID**

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

**SNMP ID:**

2.19.36.3.3.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

**Possible values:**

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

**Default:**

*empty*

**Remote-Password**

Contains the password of the remote identity.

**SNMP ID:**

2.19.36.3.3.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.19.36.3.3.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

**Possible values:**

**Yes**
**No**

**Default:**

Yes

## Digital-Signature-Profiles

Use this table to configure the profiles of the digital signature.

**SNMP ID:**

2.19.36.3.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Name**

Name of the profile.

**SNMP ID:**

2.19.36.3.4.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

**Possible values:**

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

**Default:**

DEFAULT

**Auth-Method**

Sets the authentication method for the digital signature.

**SNMP ID:**

2.19.36.3.4.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

**Possible values:**

**RSASSA-PSS**
**RSASSA-PKCS1-v1_5**

**Default:**

RSASSA-PSS

**Hash algorithms**

Sets the hash algorithms for the digital signature.

**SNMP ID:**

2.19.36.3.4.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

**Possible values:**

**SHA-512, SHA-384, SHA-256, SHA1**

**Default:**

SHA-512, SHA-384, SHA-256, SHA1

# 5.6 VPN network rules for IPv4 and IPv6

As of HiLCOS 10.12, current VPN devices allow the flexible configuration of network rules for VPN connections over IPv4 and IPv6.

## Additions to the Setup menu

### Networks

In this directory, you configure the VPN network rules for IPv4 and IPv6 connections.

**SNMP ID:**

2.19.35

**Telnet path:**

**Setup** > **VPN**

### IPv4-Rules

In this table, you configure the VPN network rules for IPv4 connections.

**SNMP ID:**

2.19.35.1

**Telnet path:**

**Setup** > **VPN** > **Networks**

### Name

Contains the name of this rule.

**SNMP ID:**

2.19.35.1.1

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv4-Rules**

**Possible values:**

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

**Default:**

*empty*

### Local-Networks

Contains the local networks to which this rule applies.

The following entries are valid:

- Name of the IP networks whose addresses 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.

Specify multiple networks by separating them with a space character.

**SNMP ID:**

2.19.35.1.2

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv4-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**Remote-Networks**

Contains the remote networks to which this rule applies.

The following entries are valid:

- Name of the IP networks whose addresses 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.

Specify multiple networks by separating them with a space character.

**SNMP ID:**

2.19.35.1.3

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv4-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**IPv4-Rule-Lists**

In this table, you collect the VPN network rules for IPv4 connections into a rule list.

**SNMP ID:**

2.19.35.2

**Telnet path:**

**Setup** > **VPN** > **Networks**

**Name**

Contains the name of this rule list.

**SNMP ID:**

2.19.35.2.1

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv4-Rules**

**Possible values:**

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

**Default:**

*empty*

### Rules

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

**SNMP ID:**

2.19.35.2.2

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv4-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

**Default:**

*empty*

## IPv6-Rules

In this table, you configure the VPN network rules for IPv6 connections.

**SNMP ID:**

2.19.35.3

**Telnet path:**

**Setup** > **VPN** > **Networks**

### Name

Contains the name of this rule.

**SNMP ID:**

2.19.35.3.1

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv6-Rules**

**Possible values:**

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

**Default:**

*empty*

**Local-Networks**

Contains the local networks to which this rule applies.

Specify multiple networks by separating them with a space character.

**SNMP ID:**

2.19.35.3.2

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv6-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**Remote-Networks**

Contains the remote networks to which this rule applies.

Specify multiple networks by separating them with a space character.

**SNMP ID:**

2.19.35.3.3

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv6-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**IPv6-Rule-Lists**

In this table, you collect the VPN network rules for IPv6 connections into a rule list.

**SNMP ID:**

2.19.35.4

**Telnet path:**

**Setup** > **VPN** > **Networks**

**Name**

Contains the name of this rule list.

**SNMP ID:**

2.19.35.4.1

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv6-Rules**

**Possible values:**

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

**Default:**

*empty*

**Rules**

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

**SNMP ID:**

2.19.35.4.2

**Telnet path:**

**Setup** > **VPN** > **Networks** > **IPv6-Rules**

**Possible values:**

Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

**Default:**

*empty*

# 5.7 Addition to the IKEv2 encryption algorithms

### DH-Groups

Contains the selection of Diffie-Hellman groups.

**SNMP ID:**

2.19.36.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**DH30**
(as of HiLCOS 10.12)
**DH29**
(as of HiLCOS 10.12)
**DH28**
(as of HiLCOS 10.12)
**DH21**
(as of HiLCOS 10.12)
**DH20**
(as of HiLCOS 10.12)
**DH19**
(as of HiLCOS 10.12)
**DH16**
**DH15**
**DH14**
**DH5**
**DH2**

**Default:**

DH14

### IKE-SA cipher list

Specifies which encryption algorithms are enabled. As of version 10.12, HiLCOS also supports AES-GCM (Galois/Counter Mode).

**SNMP ID:**

2.19.36.2.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**AES-CBC-256**
**AES-CBC-192**
**AES-CBC-128**
**3DES**
**AES-GCM-256**
(as of HiLCOS version 10.12)
**AES-GCM-192**
(as of HiLCOS version 10.12)
**AES-GCM-128**
(as of HiLCOS version 10.12)

**Default:**

AES-CBC-256

AES-GCM-256

## Child-SA cipher list

Specifies which encryption algorithms are enabled in the Child-SA. As of version 10.12, HiLCOS also supports AES-GCM (Galois/Counter Mode).

**SNMP ID:**

2.19.36.2.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Encryption**

**Possible values:**

**AES-CBC-256**
**AES-CBC-192**
**AES-CBC-128**
**3DES**
**AES-GCM-256**
(as of HiLCOS version 10.12)
**AES-GCM-192**
(as of HiLCOS version 10.12)
**AES-GCM-128**
(as of HiLCOS version 10.12)

**Default:**

AES-CBC-256

AES-GCM-256

# 5.8 IKEv2 load balancer

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer**

**Possible values:**

**Yes**

Activates the IKEv2 load balancer.

**No**

Deactivates the IKEv2 load balancer.

**Default:**

No

**Instances**

Load balancer instances are configured in the **Instances** table.

**SNMP ID:**

2.19.50.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer**

**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.

**SNMP ID:**

2.19.50.2.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Instances**

**Possible values:**

0 … 255

**Default:**

1

**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.

**SNMP ID:**

2.19.50.2.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Instances**

### Message profile

Message profile to use for this instance. The message profile contains the parameters for the status log used by the device to communicate its status information to the load balancer cluster.

**SNMP ID:**

2.19.50.2.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Instances**

**Possible values:**

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

**Default:**

DEFAULT

### 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.

**SNMP ID:**

2.19.50.2.5

**Telnet 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

**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.

**SNMP ID:**

2.19.50.2.6

**Telnet 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.

**Comment**

Contains a comment about this instance.

**SNMP ID:**

2.19.50.2.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Instances**

**Possible values:**

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

**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.

**SNMP ID:**

2.19.50.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer**

**Name**

Unique name for this profile

**SNMP ID:**

2.19.50.3.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

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

**Interface**

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

**SNMP ID:**

2.19.50.3.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

**Entries from the IPv4 networks table**

**IP address**

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

**SNMP ID:**

2.19.50.3.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

239.255.22.11

**Port**

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

**SNMP ID:**

2.19.50.3.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

0 … 65535

**Default:**

1987

**Interval**

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

**SNMP ID:**

2.19.50.3.5

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

0 … 65535

**Default:**

500

**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.

**SNMP ID:**

2.19.50.3.6

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

0 … 65535

**Default:**

3000

**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.

**SNMP ID:**

2.19.50.3.7

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

0 … 9

**Default:**

5

**Special values:**

**0**

Disables the replay detection.

**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.

**SNMP ID:**

2.19.50.3.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

0 … 255

**Default:**

15

**Key**

Shared secret for the load balancer communication log.

The secret must be the same on all of the VPN gateways in a cluster.

**SNMP ID:**

2.19.50.3.9

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

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

**Cipher**

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

**SNMP ID:**

2.19.50.3.10

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

**None**
**AES-128-GCM**
**AES-192-GCM**
**AES-256-GCM**

**Default:**

None

**HMAC**

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

**SNMP ID:**

2.19.50.3.11

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

**Possible values:**

**None**
**96 bits**
**128 bits**

**Default:**

96 bits

**Comment**

Contains a comment about this message profile.

**SNMP ID:**

2.19.50.3.12

**Telnet path:**

**Setup** > **VPN** > **IKEv2 Load Balancer** > **Instances**

**Possible values:**

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

# 6 Routing and WAN connections

## 6.1 Route monitor

### Additions to the Setup menu

#### Route monitor

In this directory, you configure the route monitor.

**SNMP ID:**

2.93.2

**Telnet path:**

**Setup** > **Routing-protocols**

**Monitor table**

In this table, you configure the route monitor.

**SNMP ID:**

2.93.2.1

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor**

**Backup peer**

Contains the name of the backup remote station.

**SNMP ID:**

2.93.2.1.1

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

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

**Default:**

*empty*

**Prefix**

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

**SNMP ID:**

2.93.2.1.2

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

Max. 43 characters from `[A-F][a-f][0-9]:./`

**Default:**

*empty*

**Rtg-Tag**

Contains the routing tag of the prefix being monitored.

**SNMP ID:**

2.93.2.1.3

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

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

**Default:**

0

**Up delay**

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

**SNMP ID:**

2.93.2.1.4

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

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

**Default:**

20

**Down delay**

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

**SNMP ID:**

2.93.2.1.5

**Telnet 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.

**Operating**

Specifies whether this backup connection is enabled.

**SNMP ID:**

2.93.2.1.6

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

**Yes**

The backup connection is enabled.

**No**

The backup connection is disabled.

**Default:**

No

**Comment**

Comment on this entry.

**SNMP ID:**

2.93.2.1.7

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor** > **Monitor-table**

**Possible values:**

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

**Default:**

*empty*

**Operating**

This action is used to enable or disable the route monitor.

**SNMP ID:**

2.93.2.2

**Telnet path:**

**Setup** > **Routing-protocols** > **Route-monitor**

**Possible values:**

**No**
The route monitor is disabled.

**Yes**
The route monitor is enabled.

**Default:**

No

# 6.2 DiffServ field enabled by default

## Additions to the Setup menu

### Routing method

Controls the analysis of ToS or DiffServ fields.

**SNMP ID:**

2.8.7.1

**Telnet 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

# 6.3 iPerf-compliant server/client

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.96

**Telnet path:**

**Setup**

**Server daemon**

This menu contains the configuration for the iPerf server daemon.

**SNMP ID:**

2.96.1

**Telnet path:**

**Setup** > **Iperf**

**Operating**

This entry is used to enable or disable the iPerf server daemon.

**SNMP ID:**

2.96.1.1

**Telnet path:**

**Setup** > **Iperf** > **Server-Daemon**

**Possible values:**

**No**

The iPerf server daemon is not active.

**Yes**

The iPerf server daemon is active.

**Default:**

No

**Transport**

Use this entry to set the transfer protocol used by the iPerf server daemon.

**SNMP ID:**

2.96.1.2

**Telnet path:**

**Setup** > **Iperf** > **Server-Daemon**

**Possible values:**

**UDP**
**TCP**

**Default:**

UDP

**Port**

Here you specify a port on which the iPerf server expects packets to arrive.

**SNMP ID:**

2.96.1.3

**Telnet path:**

**Setup** > **Iperf** > **Server-Daemon**

**Possible values:**

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

**Default:**

5001

**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.

**SNMP ID:**

2.96.2

**Telnet 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

**IPv4-Access-List**

In order restrict iPerf access to certain stations only, enter the connection data into this table.

**SNMP ID:**

2.96.3

**Telnet path:**

**Setup** > **Iperf**

**IP address**

Enter the IPv4 address of the remote station.

**SNMP ID:**

2.96.3.1

**Telnet path:**

**Setup** > **Iperf** > **IPv4-Access-List**

**Possible values:**

Max. 15 characters from `[0-9].`

**Default:**

*empty*

**Netmask**

Enter the netmask of the remote station.

**SNMP ID:**

2.96.3.2

**Telnet path:**

**Setup** > **Iperf** > **IPv4-Access-List**

**Possible values:**

Max. 15 characters from `[0-9].`

**Default:**

255,255,255,255

**Rtg-Tag**

Enter the routing tag that specifies the connection to the remote station.

**SNMP ID:**

2.96.3.3

**Telnet path:**

**Setup** > **Iperf** > **IPv4-Access-List**

**Possible values:**

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

**Default:**

0

**Comment**

Enter a descriptive comment for this entry.

**SNMP ID:**

2.96.3.4

**Telnet path:**

**Setup** > **Iperf** > **IPv4-Access-List**

**Possible values:**

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

**Default:**

*empty*

# 6.4 SLA monitor

## Additions to the Setup menu

### SLA monitor

This menu contains the settings for the SLA monitor.

**SNMP ID:**

2.45

**Telnet path:**

**Setup**

#### ICMP

This menu is used to configure the Internet Control Message Protocol (ICMP).

**SNMP ID:**

2.45.1

**Telnet path:**

**Setup** > **SLA-Monitor**

#### Name

Contains the name of the ICMP configuration.

**SNMP ID:**

2.45.1.1

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

*empty*

#### Active

This entry controls whether the ICMP profile is actually used.

**SNMP ID:**

2.45.1.2

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

**Yes**
**No**

**Default:**

Yes

**Destination**

Set an IPv4 address to which the ICMP sends diagnostic and error messages.

**SNMP ID:**

2.45.1.3

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

Max. 40 characters from `[0-9].`

**Default:**

0.0.0.0

**Rtg-Tag**

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

**SNMP ID:**

2.45.1.4

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

0

**Loopback address**

The device sees this address as its own address, which is also available even if a physical interface is disabled, for example.

**SNMP ID:**

2.45.1.5

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

Max. 56 characters from `[0-9]`

**Default:**

*empty*

### Interval

The interval in seconds in which the ICMP sends diagnostic or error messages to the specified destination.

**SNMP ID:**

2.45.1.6

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

30

### Start offset

Here you specify a startup delay for the ICMP transmissions in milliseconds.

**SNMP ID:**

2.45.1.7

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

0

### Count

Set the number of ICMP packets to be transmitted at the same time.

**SNMP ID:**

2.45.1.8

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

5

**Packet delay**

Sets delay before the ICMP packets are transmitted. Delay in milliseconds.

**SNMP ID:**

2.45.1.9

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

1000

**Packet size**

Sets the packet size for ICMP messages. The value is set in bytes.

**SNMP ID:**

2.45.1.10

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

56

**Warn-Lvl-RTT-Max**

Maximum allowable packet round-trip time before the SLA monitor emits a warning.

**SNMP ID:**

2.45.1.11

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

100

**Crit-Lvl-RTT-Max**

Maximum allowable packet round-trip time before the SLA monitor reports an error.

**SNMP ID:**

2.45.1.12

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

200

**Warn-Lvl-RTT-Avg**

Average packet round-trip time before the SLA monitor emits a warning.

**SNMP ID:**

2.45.1.13

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

80

**Crit-Lvl-RTT-Avg**

Average packet round-trip time before the SLA monitor reports an error.

**SNMP ID:**

2.45.1.14

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

170

**Warn-Lvl-Pkt-Loss-Percent**

Number of lost data packets in percent before a warning is issued.

**SNMP ID:**

2.45.1.15

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

10

**Crit-Lvl-Pkt-Loss-Percent**

Number of lost data packets in percent before an error message is issued.

**SNMP ID:**

2.45.1.16

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

20

**IP-Version**

Specifies the IP standard used for the Internet Control Message Protocol.

**SNMP ID:**

2.45.1.17

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

**Auto**
**IPv4**
**IPv6**

**Default:**

Auto

**Comment**

Comment about this ICMP configuration.

**SNMP ID:**

2.45.1.19

**Telnet path:**

**Setup** > **SLA-Monitor** > **ICMP**

**Possible values:**

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

**Default:**

*empty*

**Event count**

Number of events to be logged by the SLA monitor.

**SNMP ID:**

2.45.2

**Telnet path:**

**Setup** > **SLA-Monitor**

**Possible values:**

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

**Default:**

100

**Startup delay**

Delay time in milliseconds before monitoring is started.

**SNMP ID:**

2.45.3

**Telnet path:**

**Setup** > **SLA-Monitor**

**Possible values:**

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

**Default:**

10

# 6.5 Additional DSL-modem status values

## Additions to the Status menu

### Connection count

This entry contains the number of DSL connections since the last system reboot.

**SNMP ID:**

1.75.53

**Telnet path:**

**Status** > **VDSL**

### Connection duration

This entry contains the duration of the DSL connection since the last synchronization.

**SNMP ID:**

1.75.54

**Telnet path:**

**Status** > **VDSL**

### Connection count

This entry contains the number of DSL connections since the last system reboot.

**SNMP ID:**

1.75.25.53

**Telnet path:**

**Status** > **VDSL** > **Advanced**

### Connection duration

This entry contains the duration of the DSL connection since the last synchronization.

**SNMP ID:**

1.75.25.54

**Telnet path:**

**Status** > **VDSL** > **Advanced**

# 6.6 Displaying the mobile/cellular standards

## Additions to the Setup menu

### Mode

Select the mobile networking transmission mode here.

**SNMP ID:**

2.23.41.1.6

**Telnet 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

# 6.7 Editable VLAN assignment per Internet service provider

## Additions to the Setup menu

### VLANs

This menu contains the editable configuration of VLAN assignments for different Internet service providers.

**SNMP ID:**

2.2.60

**Telnet path:**

**Setup** > **WAN**

**Provider list**

This table contains the Internet service providers for whom VLANs should be checked in addition to VLAN 0. For this check, HiLCOS uses the "User name" entry in the PPP list under **Communication** > **Protocols**.

**SNMP ID:**

2.2.60.1

**Telnet path:**

**Setup** > **WAN** > **VLANs**

**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.

**SNMP ID:**

2.2.60.1.1

**Telnet path:**

**Setup** > **WAN** > **VLANs** > **Provider-List**

**Possible values:**

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

**Default:**

*empty*

**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 *Provider* matches the user name in the PPP list.

You have the option of specifying a single VLAN or multiple comma-separated VLANs.

**SNMP ID:**

2.2.60.1.2

**Telnet path:**

**Setup** > **WAN** > **VLANs** > **Provider-List**

**Possible values:**

Max. 64 characters from `[0-9]-,`

**Default:**

*empty*

# 6.8 Manually configuring VDSL/ADSL bandwidth

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.6.16

**Telnet path:**

**Setup** > **Interfaces** > **ADSL-Interface**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

0

**Special values:**

**0**

The value used is negotiated automatically.

## 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.

**SNMP ID:**

2.23.6.18

**Telnet path:**

**Setup** > **Interfaces** > **ADSL-Interface**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

0

**Special values:**

**0**

The value used is negotiated automatically.

## 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.

**SNMP ID:**

2.23.8.16

**Telnet path:**

**Setup** > **Interfaces** > **VDSL**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

0

**Special values:**

**0**

The value used is negotiated automatically.

## 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.

**SNMP ID:**

2.23.8.18

**Telnet path:**

**Setup** > **Interfaces** > **VDSL**

**Possible values:**

Max. 6 characters from `[0-9]`

**Default:**

0

**Special values:**

**0**

The value used is negotiated automatically.

# 6.9 The Bonjour proxy

## Additions to the Setup menu

### Bonjour proxy

This menu contains the settings for the Bonjour proxy. The Bonjour proxy allows Bonjour services to be discovered across network boundaries.

**SNMP ID:**

2.104

**Telnet path:**

**Setup**

**Operating**

This entry is used to enable or disable the Bonjour proxy.

**SNMP ID:**

2.104.1

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Query client interval**

Set the interval in minutes in which the query client requests the Bonjour services configured in the **Query client** table.

**SNMP ID:**

2.104.2

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Possible values:**

0 … 999 Minutes

**Default:**

15

**Special values:**

**0**

**Network list**

Use this table to specify the networks between which Bonjour services may be discovered.

**SNMP ID:**

2.104.3

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Name**

Specify a unique name for this table entry.

**SNMP ID:**

2.104.3.1

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

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

**Default:**

*empty*

**Active**

This entry is used to enable or disable the Bonjour proxy for the corresponding combination of client and server network.

**SNMP ID:**

2.104.3.2

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Server interface**

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

**SNMP ID:**

2.104.3.3

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

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

**Default:**

*empty*

**Client interface**

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

**SNMP ID:**

2.104.3.4

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.104.3.5

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

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

**Default:**

*empty*

**Comment**

Enter a comment about this entry.

**SNMP ID:**

2.104.3.6

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Network-List**

**Possible values:**

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

**Default:**

*empty*

### Service list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

**SNMP ID:**

2.104.4

**Telnet path:**

**Setup** > **Bonjour-Proxy**

### Name

Enter a name for this list here.

**SNMP ID:**

2.104.4.1

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Service-List**

**Possible values:**

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

**Default:**

*empty*

### 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.

**SNMP ID:**

2.104.4.2

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Service-List**

**Possible values:**

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

**Default:**

*empty*

**Services**

This table lists the default services for communicating between networks. You can extend the table according to your needs.

**SNMP ID:**

2.104.5

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Name**

Enter the service name here (e.g. "HTTP").

**SNMP ID:**

2.104.5.1

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Services**

**Possible values:**

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

**Default:**

*empty*

**Service type**

Specify the service type here (e.g. `_http._tcp.local`).

**SNMP ID:**

2.104.5.2

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Services**

**Possible values:**

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

**Default:**

*empty*

**Comment**

Enter a comment about this service.

**SNMP ID:**

2.104.5.6

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Services**

**Possible values:**

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

**Default:**

*empty*

**Query client**

The table lists the services that should be requested by the router at regular intervals.

**SNMP ID:**

2.104.6

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Name**

Specify a unique name for the corresponding entry.

**SNMP ID:**

2.104.6.1

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Query-Client**

**Possible values:**

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

**Default:**

*empty*

**Active**

Enable or disable this entry.

**SNMP ID:**

2.104.6.2

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Query-Client**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Server interface**

Here you specify the server interface to be used for the client query.

**SNMP ID:**

2.104.6.3

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Query-Client**

**Possible values:**

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

**Default:**

*empty*

**Services**

Here you specify which services should be requested.

**SNMP ID:**

2.104.6.4

**Telnet path:**

**Setup** > **Bonjour-Proxy** > **Query-Client**

**Possible values:**

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

**Default:**

*empty*

**Instance limit**

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

**SNMP ID:**

2.104.7

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Possible values:**

0 … 4294967295

**Default:**

1024

**Auto-query services**

Activate the checkbox if the Query Client should periodically query the configured service types for their availability.

**SNMP ID:**

2.104.8

**Telnet path:**

**Setup** > **Bonjour-Proxy**

**Possible values:**

**No**
**Yes**

**Default:**

Yes

# 6.10 OSPF

## Additions to the Setup menu

### OSPF

This directory enables you to configure the device for the Open Shortest Path First protocol.

**SNMP ID:**

2.93.3.

**Telnet path:**

**Setup** > **Routing-Protocols**

**OSPF instance**

This table is used to configure the OSPF instances.

**SNMP ID:**

2.93.3.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**Name**

This parameter contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.1.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

**Possible values:**

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

**Activate OSPF instance**

Activates or deactivates this OSPF instance

**SNMP ID:**

2.93.3.1.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

**Possible values:**

**0**

Disabled

**1**

Activated

**Default:**

0

**Router ID**

The 32-bit router ID of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

**SNMP ID:**

2.93.3.1.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Routing tag**

Contains the routing tag assigned to this instance.

**SNMP ID:**

2.93.3.1.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

**Possible values:**

0 … 65535

**Advertise default route**

Specifies whether this router should advertise or propagate the default route in this instance.

**SNMP ID:**

2.93.3.1.5

**Telnet 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

**OSPF areas**

This table is used to configure the OSPF areas.

**SNMP ID:**

2.93.3.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

This parameter contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.2.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

**Possible values:**

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

**Area ID**

The area ID (displayed as an IPv4 address) identifies the area.

**SNMP ID:**

2.93.3.2.2

**Telnet 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.

**Area type**

This parameter describes the type of the area.

**SNMP ID:**

2.93.3.2.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

**Possible values:**

**Normal**
**Stub**

**Default:**

Normal

**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.

**SNMP ID:**

2.93.3.2.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

**Possible values:**

0 … 4294967295

**Area address aggregation**

This table is used to configure the area address aggregation.

**SNMP ID:**

2.93.3.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

This parameter contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.3.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

**Possible values:**

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

**Area ID**

Contains the ID of the area.

**SNMP ID:**

2.93.3.3.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**IP address**

This parameter contains the IPv4 address.

**SNMP ID:**

2.93.3.3.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**IP netmask**

This parameter contains the IPv4 subnet mask.

**SNMP ID:**

2.93.3.3.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

**Possible values:**

IPv4 netmask `[0-9.]`

**Advertise**

Enables or disables the advertisement of this address aggregation.

**SNMP ID:**

2.93.3.3.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

**Possible values:**

**No**

Advertising disabled

**Yes**

Advertising enabled

**Default:**

No

**OSPF interfaces**

Specifies the interfaces on which OSPF is operated.

**SNMP ID:**

2.93.3.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF interface**

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

**SNMP ID:**

2.93.3.4.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **OSPF-Interfaces**

**Possible values:**

Characters from the following character set: `[a-z A-Z 0-9 .]`

**OSPF instance**

This parameter contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.4.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

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

**Area ID**

Contains the ID of the area.

**SNMP ID:**

2.93.3.4.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Interface type**

Contains the interface type.

**SNMP ID:**

2.93.3.4.4

**Telnet 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.

**Non-Broadcast Multi- Access (NBMA)**

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.

**Default:**

Broadcast

**Output cost**

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.

**SNMP ID:**

2.93.3.4.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

0 … 4294967295

**Retransmit interval**

Contains the number of seconds between retransmissions.

**SNMP ID:**

2.93.3.4.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

0 … 4294967295

**Transmit delay**

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

**SNMP ID:**

2.93.3.4.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

0 … 4294967295

### 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.

**SNMP ID:**

2.93.3.4.8

**Telnet 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.

### Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

**SNMP ID:**

2.93.3.4.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

0 … 4294967295

### 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.

**SNMP ID:**

2.93.3.4.10

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

0 … 4294967295

**Authentication type**

Authentication method used for this interface.

**SNMP ID:**

2.93.3.4.11

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

**Null**
**Simple password**
**Cryptographic MD5**

**Default:**

Null

**Authentication key**

Authentication key for this network in the case that the authentication type **Null** is used.

**SNMP ID:**

2.93.3.4.12

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Interfaces**

**Possible values:**

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

**Passive**

Defines whether OSPF works actively or passively on this interface.

**SNMP ID:**

2.93.3.4.13

**Telnet 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

**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.

**SNMP ID:**

2.93.3.4.14

**Telnet path:**

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.93.3.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.5.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

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

**Transit area ID**

Defines the area ID of the transit area.

**SNMP ID:**

2.93.3.5.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Router ID**

Defines the router ID of the router at the remote end of the virtual link.

**SNMP ID:**

2.93.3.5.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Retransmit interval**

Contains the number of seconds between retransmissions.

**SNMP ID:**

2.93.3.5.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

0 … 4294967295

### Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

**SNMP ID:**

2.93.3.5.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

0 … 4294967295

### 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.

**SNMP ID:**

2.93.3.5.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

0 … 4294967295

### Authentication type

Authentication method used for this interface.

**SNMP ID:**

2.93.3.5.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

**Null**
**Simple password**
**Cryptographic MD5**

**Default:**

Null

### Authentication key

Authentication key for this network in the case that the authentication type **Null** is used.

**SNMP ID:**

2.93.3.5.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Virtual-Links**

**Possible values:**

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

### 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.

**SNMP ID:**

2.93.3.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

### OSPF instance

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.6.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

**Possible values:**

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

**OSPF interface**

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

**SNMP ID:**

2.93.3.6.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

**Possible values:**

Characters from the following character set: `[a-z A-Z 0-9 .]`

**IP address**

Contains the IPv4 address of the neighbor router at the remote end.

**SNMP ID:**

2.93.3.6.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Request interval**

Defines the interval in which Hello messages are sent to this router.

**SNMP ID:**

2.93.3.6.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

**Possible values:**

0 … 4294967295

**Special values:**

**0**

Disables the transmission of Hello messages.

**Eligible as default router**

Specifies whether the local device itself is selectable as default router.

**SNMP ID:**

2.93.3.6.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.93.3.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.7.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

**Possible values:**

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

**OSPF interface**

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

**SNMP ID:**

2.93.3.7.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

**Possible values:**

Characters from the following character set: `[a-z A-Z 0-9 .]`

**IP address**

Contains the IPv4 address of the neighbor router at the remote end.

**SNMP ID:**

2.93.3.7.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

**Possible values:**

IPv4 address `[0-9.]`

**Default:**

0.0.0.0

**Request interval**

Defines the interval in which Hello messages are sent to this router.

**SNMP ID:**

2.93.3.7.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

**Possible values:**

0 … 4294967295

**Special values:**

**0**

Disables the transmission of Hello messages.

#### BGP

in the **BGP** menu you configure the redistribution of routes that were learned dynamically from the Border Gateway Protocol.

**SNMP ID:**

2.93.3.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

#### OSPF instance

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.8.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **BGP**

**Possible values:**

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

#### BGP instance

Contains the name of the BGP instance.

**SNMP ID:**

2.93.3.8.2

**Telnet path:**

**Routing-Protocols** > **OSPF** > **BGP**

**Possible values:**

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

**Metric source**

Specifies which source is used to set the OSPF metric.

**SNMP ID:**

2.93.3.8.3

**Telnet path:**

**Routing-Protocols** > **OSPF** > **BGP**

**Possible values:**

**Constant**

Uses a user-defined constant metric.

**Protocol**

Uses the "local preference" value of the BGP prefix.

**Default:**

Constant

**Constant metric**

Contains the constant for the OSPF metric of the imported routes.



The metric source must first have been set to **Constant**.

**SNMP ID:**

2.93.3.8.4

**Telnet path:**

**Routing-Protocols** > **OSPF** > **BGP**

**Possible values:**

0 … 4294967295

**Path type**

Specifies the type of routes that were imported into OSPF.

**SNMP ID:**

2.93.3.8.5

**Telnet path:**

**Routing-Protocols** > **OSPF** > **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.

**External route tag**

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

**SNMP ID:**

2.93.3.8.6

**Telnet path:**

**Routing-Protocols** > **OSPF** > **BGP**

**Possible values:**

0 … 4294967295

**Connected**

Routes that are automatically entered into the routing table by the operating system are configured under **Connected**.

**SNMP ID:**

2.93.3.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.9.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Connected**

**Possible values:**

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

**Metric source**

Specifies which source is used to set the OSPF metric.

**SNMP ID:**

2.93.3.9.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Connected**

**Possible values:**

**Constant**

Uses a user-defined constant metric.

**Protocol**

Uses a value set automatically.

**Default:**

Constant

**Constant metric**

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

**SNMP ID:**

2.93.3.9.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Connected**

**Possible values:**

0 … 4294967295

**Path type**

Specifies the type of routes that were imported into OSPF.

**SNMP ID:**

2.93.3.9.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **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.

**External route tag**

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

**SNMP ID:**

2.93.3.9.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Connected**

**Possible values:**

0 … 4294967295

**Static**

Routes that the user manually enters into the routing table are configured in the menu **Static**.

**SNMP ID:**

2.93.3.10

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF**

**OSPF instance**

Contains the name of the OSPF instance.

**SNMP ID:**

2.93.3.10.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Static**

**Possible values:**

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

**Metric source**

Specifies which source is used to set the OSPF metric.

**SNMP ID:**

2.93.3.10.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Static**

**Possible values:**

**Constant**

Uses a user-defined constant metric.

**Protocol**

Uses a value set automatically.

**Default:**

Constant

**Constant metric**

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

**SNMP ID:**

2.93.3.10.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Static**

**Possible values:**

0 … 4294967295

**Path type**

Specifies the type of routes that were imported into OSPF.

**SNMP ID:**

2.93.3.10.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **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.

**External route tag**

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

**SNMP ID:**

2.93.3.10.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **OSPF** > **Static**

**Possible values:**

0 … 4294967295

# 7 IPv6

## 7.1 IPv6 support for (S)NTP client and server

### Additions to the Setup menu

#### 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.

**SNMP ID:**

2.26.3

**Telnet path:**

**Setup** > **NTP**

**Possible values:**

**No**

The send mode is disabled.

**Yes**

The send mode is enabled.

**Default:**

No

## 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.

**SNMP ID:**

2.26.11.1

**Telnet path:**

**Setup** > **NTP** > **RQ-Address**

**Possible values:**

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

**Default:**

*empty*

## 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

**SNMP ID:**

2.26.11.2

**Telnet path:**

**Setup** > **NTP** > **RQ-Address**

**Possible values:**

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

**Default:**

*empty*

# 7.2 Support for SNTP option in the DHCPv6 client

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.70.3.2.1.10

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

**Possible values:**

**0**

No

**1**

Yes

**Default:**

0

# 7.3 Support of prefix hint in the DHCPv6 client

## Additions to the Setup menu

### PD hint

Here you specify whether the DHCPv6 client requests a desired prefix length from the DHCPv6 server.

**SNMP ID:**

2.70.3.2.1.11

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

**Possible values:**

Three characters from the following character set: `[0-9]`

# 7.4 DHCPv6 options

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.70.3.1.8

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server**

**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

**SNMP ID:**

2.70.3.1.8.1

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

**Possible values:**

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

**Option code**

Enter the code of your DHCPv6 option here.

**SNMP ID:**

2.70.3.1.8.2

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

**Possible values:**

0 … 65535

**Default:**

0

**Option type**

Select the type of your DHCPv6 option here.

**SNMP ID:**

2.70.3.1.8.3

**Telnet 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**.

**Option value**

Enter the contents of your DHCPv6 option here. The content must be formatted according to the selected option type.

**SNMP ID:**

2.70.3.1.8.4

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

**Possible values:**

Depending on the option type, characters from:

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

# 8 Diagnosis

## 8.1 Layer-7 application detection

### Additions to the Setup menu

#### Layer-7 app detection

This menu is used to configure layer-7 application detection.

**SNMP ID:**

2.101

**Telnet path:**

**Setup**

**Operating**

This entry is used to enable or disable layer-7 application detection.

**SNMP ID:**

2.101.1

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**Possible values:**

**No**
**Yes**

**Default:**

No

#### IP port applications

Set the target ports for the layer-7 application detection, or add new entries to the table.

**SNMP ID:**

2.101.2

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

#### Application name

Specify a unique name for this application.

**SNMP ID:**

2.101.2.1

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **IP-Port-Applications**

**Possible values:**

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

**Default:**

*empty*

**Targets**

Define targets for this application.

Specify multiple targets with a comma-separated list.

**SNMP ID:**

2.101.2.2

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **IP-Port-Applications**

**Possible values:**

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

**Default:**

*empty*

**Ports**

Specify the ports to be tracked.

**SNMP ID:**

2.101.2.3

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **IP-Port-Applications**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.101.4

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**Port**

This entry contains the name of the port selected from the table.

**SNMP ID:**

2.101.4.2

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **Port-Table**

**Traffic tracking**

This entry is used to enable or disable the tracking of traffic for this port.

**SNMP ID:**

2.101.4.3

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **Port-Table**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Status-Update-In-Minute**

This entry sets an interval in minutes when the usage statistics are updated.

**SNMP ID:**

2.101.5

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**Possible values:**

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

**Default:**

60

#### Max queue length

This entry specifies the maximum queue length for the usage statistics.

**SNMP ID:**

2.101.6

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**Possible values:**

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

**Default:**

10000

#### Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

**SNMP ID:**

2.101.7

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

#### HTTP-HTTPS tracking

In this menu, specify the entries for the tracking of HTTP / HTTPS connections.

**SNMP ID:**

2.101.8

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

#### Application name

Name for the tracking of HTTP / HTTPS connections (e.g. youtube).

**SNMP ID:**

2.101.8.1

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

**Possible values:**

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

**Default:**

*empty*

**Targets**

Here you specify the targets for the tracking of HTTP / HTTPS connections (e.g. youtube).

Specify multiple targets in a comma-separated list (e.g. youtube, googlevideo, ytimg)

**SNMP ID:**

2.101.8.2

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

**Possible values:**

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

**Default:**

*empty*

**Prio**

Set the priority of HTTP/HTTPS tracking by the layer-7 application detection.

**SNMP ID:**

2.101.8.3

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

**Possible values:**

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

**Default:**

0

**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.

**SNMP ID:**

2.101.11

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**VLAN-ID**

Use this entry to specify a VLAN ID.

**SNMP ID:**

2.101.11.1

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **VLAN**

**Possible values:**

0 … 65535

**Default:**

0

**Track user**

With this entry you enable or disable the collection of user-specific data (user or client name and MAC address).

**SNMP ID:**

2.101.11.2

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **VLAN**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Tracking active**

This entry is used to enable or disable the collection of general or application-specific data.

**SNMP ID:**

2.101.11.3

**Telnet path:**

**Setup** > **Layer-7-App-Detection** > **VLAN**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Save-In-Min**

Specify the interval in minutes for storing the usage statistics of the layer-7 application detection.

**SNMP ID:**

2.101.12

**Telnet path:**

**Setup** > **Layer-7-App-Detection**

**Possible values:**

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

**Default:**

3600

# 8.2 SYSLOG messaging via TCP

## Additions to the Setup menu

### Port

This entry contains the port used for SYSLOG.

**SNMP ID:**

2.22.2.8

**Telnet path:**

**Setup** > **SYSLOG** > **Server**

**Possible values:**

**514**

TCP/UDP

**Default:**

514

### Protocol

This entry contains the protocol used for SYSLOG.

**SNMP ID:**

2.22.2.9

**Telnet path:**

**Setup** > **SYSLOG** > **Server**

**Possible values:**

**TCP**
**UDP**

**Default:**

UDP

# 9 RADIUS

## 9.1 Automatic clean-up of access information on the RADIUS server

### Additions to the Setup menu

#### Auto-Cleanup-Accounting-Totals

Closed accounting sessions are deleted if the function "RADIUS cleanup user table" has removed the related RADIUS account.

**SNMP ID:**

2.25.10.18

**Telnet path:**

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

**Possible values:**

**No**

Accounting information is not automatically deleted.

**Yes**

Accounting information is deleted automatically.

**Default:**

Yes

# 9.2 Dynamic authorization by RADIUS CoA (Change of Authorization)

## Additions to the Setup menu

### Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176* .

**SNMP ID:**

2.25.19

**Operating**

This entry enables or disables the dynamic authorization by RADIUS.

**SNMP ID:**

2.25.19.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Port**

This entry specifies the port on which CoA messages are accepted.

**SNMP ID:**

2.25.19.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

3799

**WAN access**

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

**SNMP ID:**

2.25.19.3

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Clients**

All of the CoA clients that send messages to the NAS are entered into this table.

**SNMP ID:**

2.25.19.4

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

## HostName

This entry contains the unique identifier of the client that sends messages to the NAS.

**SNMP ID:**

2.25.19.4.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Clients**

**Possible values:**

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

**Default:**

*empty*

## Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

**SNMP ID:**

2.25.19.4.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Clients**

**Possible values:**

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

**Default:**

*empty*

**Forward-Servers**

To forward CoA messages, the forwarding servers are specified here.

**SNMP ID:**

2.25.19.5

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

## Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

**SNMP ID:**

2.25.19.5.1

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

## HostName

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

**SNMP ID:**

2.25.19.5.2

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

### Port

This entry contains the port for communications with the forwarding server.

**SNMP ID:**

2.25.19.5.3

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

0

### Secret

This entry specifies the secret required to access the forwarding server.

**SNMP ID:**

2.25.19.5.4

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

### 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.

**SNMP ID:**

2.25.19.5.5

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

**Possible values:**

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

**Default:**

*empty*

**Default realm**

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

**SNMP ID:**

2.25.19.6

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

*empty*

**Empty realm**

This realm is used when the specified username does not contain a realm.

**SNMP ID:**

2.25.19.7

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

**Possible values:**

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

**Default:**

*empty*

**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 HiLCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

**SNMP ID:**

2.25.19.8

**Telnet path:**

**Setup** > **RADIUS** > **Dyn-Auth**

# 9.3 Support of tunnel-password and LCS-routing-tag attributes

## Additions to the Setup menu

### Tunnel-Password

This entry sets the connection password for each user.

**SNMP ID:**

2.25.10.7.23

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

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

**Default:**

*empty*

### LCS-Routing-Tag

Specify the routing tag for this connection.

**SNMP ID:**

2.25.10.7.24

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

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

**Default:**

0

# 9.4 Restricting WAN access to the RADIUS server

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.25.10.22

**Telnet 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

# 10. Interface bundling with LACP

## 10.1 Configuring the LACP interfaces

### Additions to the Setup menu

#### LACP

This menu is used to configure the Link Aggregation Control Protocol (LACP).

**SNMP ID:**

2.4.13.12

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling**

**Interfaces**

Select an interface bundle here.

**SNMP ID:**

2.4.13.12.1

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **LACP**

**Possible values:**

**BUNDLE-1**
Interface bundle 1

**BUNDLE-2**
Interface bundle 2

**Interface**

Use this menu to access the advanced features.

**SNMP ID:**

2.4.13.12.1.1

**Telnet 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

**System-Priority**

Set the system priority here.

**SNMP ID:**

2.4.13.12.1.2

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

**Possible values:**

Multiples of 4096 `[0-9]`

**Default:**

32768

**Key**

Here, you assign a number as an identifier for the bundle.

**SNMP ID:**

2.4.13.12.1.3

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

**Possible values:**

1 … 54

**Default:**

42

**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.

**SNMP ID:**

2.4.13.12.1.4

**Telnet 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

**Port priority A**

Here you set the status values for port priority A.

**SNMP ID:**

2.4.13.12.1.5

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

**Possible values:**

Multiples of 4096 `[0-9]`

**Default:**

32768

**Port priority B**

Here you set the status values for port priority A.

**SNMP ID:**

2.4.13.12.1.6

**Telnet path:**

**Setup** > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

**Possible values:**

Multiples of 4096 `[0-9]`

**Default:**

32768

# 11 Other Services

## 11.1 DHCP lease time per network

### Additions to the Setup menu

#### 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.

**SNMP ID:**

2.10.20.20

**Telnet path:**

**Setup** > **DHCP** > **Network-List**

**Possible values:**

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

**Default:**

0

**Special values:**

**0**

There is no limit on the lease time that the DHCP client may request.

#### 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.

**SNMP ID:**

2.10.20.21

**Telnet path:**

**Setup** > **DHCP** > **Network-List**

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

**Default:**

0

**Special values:**

**0**

There is no limit on the lease time that can be assigned to the DHCP client.

# 11.2 DHCP lease RADIUS accounting

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.10.23

**Telnet path:**

**Setup** > **DHCP**

**Operating**

Enables or disables the RADIUS accounting on this DHCP network.

**SNMP ID:**

2.10.23.1

**Telnet 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

**Interim Interval**

Here you specify the time interval in seconds after which the DHCP server sends a `RADIUS interim update` to the accounting server.

**SNMP ID:**

2.10.23.2

**Telnet path:**

**Setup** > **DHCP** > **RADIUS-Accounting**

**Possible values:**

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

**Network list**

This table contains the IP networks for the RADIUS accounting.

**SNMP-ID:**

2.10.23.20

**Pfad Telnet:**

**Setup** > **DHCP** > **RADIUS-Accounting**

**Network name**

Contains the name of the network.

**SNMP-ID:**

2.10.23.20.1

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Server host name**

Enter the host name of the RADIUS accounting server here.

**SNMP-ID:**

2.10.23.20.2

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Accnt.-Port**

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port „1813".

**SNMP-ID:**

2.10.23.20.3

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

1813

**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.

**SNMP-ID:**

2.10.23.20.4

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**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.

**SNMP-ID:**

2.10.23.20.5

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Protocol**

Use this entry to specify the protocol used to communicate with the RADIUS accounting server.

**SNMP-ID:**

2.10.23.20.6

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

**RADIUS**
**RADSEC**

**Default-Wert:**

RADIUS

**Attribute-Values**

HiLCOS 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`.

**SNMP-ID:**

2.10.23.20.7

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Backup server hostname**

Enter the host name of the backup server here.

**SNMP-ID:**

2.10.23.20.12

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Backup-Accnt.-Port**

Here you enter the backup port used by the backup RADIUS accounting server.

**SNMP-ID:**

2.10.23.20.13

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

0

**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.

**SNMP-ID:**

2.10.23.20.14

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Backup-Loopback-Address**

Specify a loopback address for the backup RADIUS accounting server.

**SNMP-ID:**

2.10.23.20.15

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Backup-Protocol**

Use this entry to specify the protocol used to communicate with the backup RADIUS accounting server.

**SNMP-ID:**

2.10.23.20.16

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

**RADIUS**
**RADSEC**

**Default-Wert:**

RADIUS

**Backup attribute values**

Here you specify the attribute values for the backup RADIUS accounting server.

**SNMP-ID:**

2.10.23.20.17

**Pfad Telnet:**

**Setup** > **DHCP** > > **RADIUS-Accounting** > **Network-List**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

# 11.3 SNMPv3 support

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.9.27

**Telnet path:**

**Setup** > **SNMP**

**Name**

Enter a descriptive name for this SNMP community.

**SNMP ID:**

2.9.27.1

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Security-Name**

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

**SNMP ID:**

2.9.27.3

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

#### Status

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

**SNMP ID:**

2.9.27.8

**Telnet path:**

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

**Possible values:**

**Active**

The community is enabled.

**Inactive**

The community is disabled.

**Default:**

Active

### 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.

**SNMP ID:**

2.9.28

**Telnet path:**

**Setup** > **SNMP**

#### Security-Model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in HiLCOS 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.

**SNMP ID:**

2.9.28.1

**Telnet 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)

**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.

**SNMP ID:**

2.9.28.2

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Group-Name**

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

**SNMP ID:**

2.9.28.3

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Status**

Activates or deactivates this group configuration.

**SNMP ID:**

2.9.28.5

**Telnet path:**

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

**Possible values:**

**Active**
**Down**

**Default:**

Active

## Access

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

**SNMP ID:**

2.9.29

**Telnet path:**

**Setup** > **SNMP**

**Group-Name**

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

**SNMP ID:**

2.9.29.1

**Telnet path:**

**Setup** > **SNMP** > **Access**

**Possible values:**

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

**Default:**

*empty*

**Security model**

Activate the appropriate security model here.

**SNMP ID:**

2.9.29.3

**Telnet 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

**Read-View-Name**

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

**SNMP ID:**

2.9.29.5

**Telnet path:**

**Setup** > **SNMP** > **Access**

**Possible values:**

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

**Default:**

*empty*

**Write-View-Name**

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

**SNMP ID:**

2.9.29.6

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Accesses**

**Possible values:**

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

**Default:**

*empty*

**Notify-View-Name**

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

**SNMP ID:**

2.9.29.7

**Telnet path:**

**Setup** > **SNMP** > **Access**

**Possible values:**

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

**Default:**

*empty*

**Status**

Activates or deactivates this entry.

**SNMP ID:**

2.9.29.9

**Telnet path:**

**Setup** > **SNMP** > **Access**

**Possible values:**

**Active**
**Down**

**Default:**

Active

**Min-Security-Level**

Specify the minimum security level for access and data transfer.

**SNMP ID:**

2.9.29.10

**Telnet 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

## 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.

**SNMP ID:**

2.9.30

**Telnet path:**

**Setup** > **SNMP**

### View-Name

Give the view a descriptive name here.

**SNMP ID:**

2.9.30.1

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

### 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**.

**SNMP ID:**

2.9.30.2

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Type**

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

**SNMP ID:**

2.9.30.4

**Telnet path:**

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

**Possible values:**

**Included**

This setting outputs MIB values.

**Excluded**

This setting blocks the output of MIB values.

**Default:**

Included

**Status**

Activates or deactivates this view.

**SNMP ID:**

2.9.30.6

**Telnet path:**

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

**Possible values:**

**Active**
**Down**

**Default:**

Active

## SNMPv3-Users

This menu contains the user configuration.

**SNMP ID:**

2.9.32

**Telnet path:**

**Setup** > **SNMP**

**User name**

Specify the SNMPv3 user name here.

**SNMP ID:**

2.9.32.2

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Users**

**Possible values:**

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

**Default:**

*empty*

**Authentication-Protocol**

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

**SNMP ID:**

2.9.32.5

**Telnet 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).

**Default:**

HMAC-SHA

**Authentication-Password**

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

**SNMP ID:**

2.9.32.6

**Telnet path:**

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

**Possible values:**

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

**Default:**

*empty*

**Privacy-Protocol**

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

**SNMP ID:**

2.9.32.8

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Users**

**Possible values:**

**None**

Communication is not encrypted.

**DES**

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

**AES128**

Encryption is performed with AES128 (key length 128 bits).

**AES192**

Encryption is performed with AES192 (key length 192 bits).

**AES256**

Encryption is performed with AES256 (key length 256 bits)

**Default:**

AES128

**Privacy-Password**

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

**SNMP ID:**

2.9.32.9

**Telnet path:**

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

**Possible values:**

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

**Default:**

*empty*

**Status**

Activates or deactivates this user.

**SNMP ID:**

2.9.32.13

**Telnet path:**

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

**Possible values:**

**Active**
**Down**

**Default:**

Active

## SNMPv3-Notifiers

This menu contains the table with the SNMPv3 notifications.

**SNMP ID:**

2.9.33

**Telnet path:**

**Setup** > **SNMP**

**Notify-Name**

Enter a name for this notifier here.

**SNMP ID:**

2.9.33.1

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Notifiers**

**Possible values:**

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

**Default:**

*empty*

**Notify-Tag**

Enter the notifier tag here.

**SNMP ID:**

2.9.33.2

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Notifiers**

**Possible values:**

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

**Default:**

*empty*

**Notify-Type**

Contains the notification types.

**SNMP ID:**

2.9.33.3

**Telnet path:**

**Setup** > **SNMP** > **SNMPv3-Notifiers**

**Possible values:**

**NOTIFICATION-TRAP**

**Default:**

NOTIFICATION-TRAP

## 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.

**SNMP ID:**

2.9.34

**Telnet path:**

**Setup** > **SNMP**

**Target-Address-Name**

Specify the target address name here.

**SNMP ID:**

2.9.34.1

**Telnet path:**

**Setup** > **SNMP** > **Target-Address**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.9.34.3

**Telnet path:**

**Setup** > **SNMP** > **Target-Address**

**Possible values:**

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

**Default:**

*empty*

**Target-Tag-List**

Contains a tag list for defining target addresses for specific tasks.

**SNMP ID:**

2.9.34.6

**Telnet path:**

**Setup** > **SNMP** > **Target-Address**

**Possible values:**

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

**Default:**

*empty*

**Parameters-Name**

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

**SNMP ID:**

2.9.34.7

**Telnet path:**

**Setup** > **SNMP** > **Target-Address**

**Possible values:**

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

**Default:**

*empty*

## Target-Params

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

**SNMP ID:**

2.9.35

**Telnet path:**

**Setup** > **SNMP**

**Name**

Give the entry a descriptive name here.

**SNMP ID:**

2.9.35.1

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Message-Processing-Model**

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

**SNMP ID:**

2.9.35.2

**Telnet path:**

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

**Possible values:**

**SNMPv1**
**SNMPv2c**
**SNMPv3**

**Default:**

SNMPv3

**Security model**

Use this entry to specify the security model.

**SNMP ID:**

2.9.35.3

**Telnet path:**

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

**Possible values:**

**SNMPv1**
**SNMPv2**
**SNMPv3(USM)**

**Default:**

SNMPv3(USM)

**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.

**SNMP ID:**

2.9.35.4

**Telnet path:**

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

**Possible values:**

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

**Default:**

*empty*

**Security-Level**

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

**SNMP ID:**

2.9.35.5

**Telnet 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

## Notification-Server-Enable

This entry specifies whether the server notification is enabled or disabled.

**SNMP ID:**

2.9.36

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**No**

Server notification is disabled.

**Yes**

Server notification is enabled.

**Default:**

No

## Admitted-Protocols

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

**SNMP ID:**

2.9.37

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**SNMPv1**
**SNMPv2**
**SNMPv3**

**Default:**

SNMPv1

SNMPv2

SNMPv3

## Allow admins

Enable this option if registered administrators should also have access via SNMPv3.

**SNMP-ID:**

2.9.38

**Pfad Telnet:**

**Setup** > **SNMP**

**Mögliche Werte:**

**No**
**Yes**

**Default-Wert:**

Yes

### SNMPv3-Admin-Authentication

Sets the authorization method for administrators.

This value cannot be modified.

**SNMP ID:**

2.9.39

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**AUTH-HMAC-SHA**

**Default:**

AUTH-HMAC-SHA

### SNMPv3-Admin-Privacy

Specifies the encryption settings for administrators.

This value cannot be modified.

**SNMP ID:**

2.9.40

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**AES256**

**Default:**

AES256

## Operating

This entry enables or disables SNMP traps. Clear the checkbox to disable SNMP traps.

**SNMP ID:**

2.9.41

**Telnet path:**

**Setup** > **SNMP**

**Possible values:**

**No**
**Yes**

**Default:**

Yes

# 11.4 Logging DNS queries with SYSLOG

## Additions to the Setup menu

### Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

**SNMP ID:**

2.17.20

**Telnet path:**

**Setup** > **DNS**

**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`)

**SNMP ID:**

2.17.20.1

**Telnet 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

**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.

**SNMP ID:**

2.17.20.2

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

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

**Log source**

Contains the log source as displayed in the SYSLOG messages.

**SNMP ID:**

2.17.20.3

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

**System**
**Login**
**System time**
**Console login**
**Connections**
**Accounting**
**Administration**
**Router**

**Default:**

Router

**Log level**

Contains the priority that is shown in the SYSLOG messages.

**SNMP ID:**

2.17.20.4

**Telnet path:**

**Setup** > **DNS** > **Syslog**

**Possible values:**

**Emergency**
**Alert**
**Critical**
**Error**
**Warning**
**Notice**
**Info**
**Debug**

**Default:**

Notice

**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.

**SNMP ID:**

2.17.20.5

**Telnet 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**

### Source

Here you select which source is entered in the SYSLOG messages.

**SNMP ID:**

2.22.2.3

**Telnet path:**

**Setup** > **SYSLOG** > **SYSLOG table**

**Possible values:**

**None**
**System**
**Login**
**System time**
**Console login**
**Connections**
**Accounting**
**Administration**
**Router**

**Default:**

None

### Level

Here you select the source that is entered in the SYSLOG messages. Multiple entries can be selected.

**SNMP ID:**

2.22.2.4

**Telnet path:**

**Setup** > **SYSLOG** > **SYSLOG table**

**Possible values:**

**None**
**Alert**
**Error**
**Warning**
**Info**
**Debug**

**Default:**

None

## 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.

**SNMP ID:**

2.22.2.7

**Telnet path:**

**Setup** > **SYSLOG** > **SYSLOG table**

**Possible values:**

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

## Facility

The mapping of sources to specific facilities.

**SNMP ID:**

2.22.3.2

**Telnet 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**

# 11.5 Time server for the local network

## Additions to the Setup menu

### Authentication

Enables or disables MD5 authentication for the client.

**SNMP ID:**

2.26.11.3

**Telnet path:**

**Setup** > **NTP** > **RQ-Address**

**Possible values:**

**No**

Disabled

**Yes**

Enabled

**Default:**

No

### Key-ID

Identifies the key ID used for the client for MD5 authentication.

**SNMP ID:**

2.26.11.4

**Telnet path:**

**Setup** > **NTP** > **RQ-Address**

**Possible values:**

1 … 65535

## Authentication

Enables or disables MD5 authentication for the server.

**SNMP ID:**

2.26.13

**Telnet path:**

**Setup** > **NTP**

**Possible values:**

**No**

Disabled

**Yes**

Enabled

**Default:**

No

## Key

Configures the table **Authentication-Keys**.

**SNMP ID:**

2.26.14

**Telnet path:**

**Setup** > **NTP**

**Key-ID**

Identifies the key ID used for the server for MD5 authentication.

**SNMP ID:**

2.26.14.1

**Telnet path:**

**Setup** > **NTP** > **Authentication-Keys**

**Possible values:**

1 … 65535

**Key**

This entry contains the value of the key.

**SNMP ID:**

2.26.14.2

**Telnet path:**

**Setup** > **NTP** > **Authentication-Keys**

**Possible values:**

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

### Server-Trusted-Keys

Contains the list of trusted keys (comma-separated list of key numbers).

**SNMP ID:**

2.26.15

**Telnet path:**

**Setup** > **NTP**

**Possible values:**

Max. 63 characters from `[0-9,]`

### Network list

This list contains the networks that your device uses as a time server.

**SNMP ID:**

2.26.16

**Telnet path:**

**Setup** > **NTP**

**Network name**

Defines the name of the network on which the NTP server is to be activated.

**SNMP ID:**

2.26.16.1

**Telnet path:**

**Setup** > **NTP** > **Networklist**

**Possible values:**

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

**Server-Operating**

Defines whether the NTP server is enabled on the selected network.

**SNMP ID:**

2.26.16.2

**Telnet path:**

**Setup** > **NTP** > **Networklist**

**Possible values:**

**No**
Disabled

**Yes**
Enabled

**Default:**

No

## Server-WAN-Access

Configures WAN access to your device.

**SNMP ID:**

2.26.17

**Telnet 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.

# 11.6 Simple Network Management Protocol (SNMP)

## Additions to the Setup menu

### Authentication-Protocol

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

As of HiLCOS 10.12, you can use hash algorithms with a hash length of 224 bits and more.

**SNMP ID:**

2.9.32.5

**Telnet 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

# Addendum

## HiLCOS Rel. 10.12-RU7

# 1 Addendum to HiLCOS Rel. 10.12-RU7

This document describes the changes and enhancements in HiLCOS Rel. 10.12-RU7 since the previous version.

# 2 WLAN

## 2.1 Buffer Flush

### 2.1.1 Hardware Buffer Flush

#### Additions to the Setup menu

**Hardware-Buffer-Flush**
Allows the user to flush transmit Hardware buffers on BAT devices. Per default flushing is disabled. The user can set the number of consecutive flushes.

---

Emptying the buffer may lead to packet loss. This can cause retransmission of packets from the external application.

This command is only available on devices that act as a WLAN Client.

---

**SNMP ID:**

2.12.256

**Telnet path:**

**Setup** > **WLAN > Hardware-Buffer-Flush**

**Possible values:**

Max. 3 characters from
[0-9]

**Default:**

0

**Example 1:** Flush the Hardware Buffers 3 times after a StuckTransmitter Error has occured.

*set /Setup/WLAN/Hardware-Buffer-Flush 3*

**Example 2:** Disable this functionality.

*set /Setup/WLAN/Hardware-Buffer-Flush 0*

## 2.1.2 Software Buffer Flush

### Additions to the Setup menu

**Software-Buffer-Flush**
Allows the user to flush transmit Software buffers on BAT devices. Per default flushing is disabled. The user can set the duration that a flush shall take in milliseconds.

Emptying the buffer may lead to packet loss. This can cause retransmission of packets from the external application.

Flushing of software buffers is only active if flushing of hardware buffers is active.

This command is only available on devices which act as WLAN client.

**SNMP ID:**

2.12.257

**Telnet path:**

**Setup** > **WLAN > Software-Buffer-Flush**

**Possible values:**

Max. 10 characters from
[0-9]
Unit is in milliseconds (ms)

**Default:**

0

**Example 1:** Flush the Software Buffers for a duration of 2000 milliseconds after a StuckTransmitter Error has occured.

*set /Setup/WLAN/Software-Buffer-Flush 2000*

**Example 2:** Disable this functionality.

*set /Setup/WLAN/Software-Buffer-Flush 0*

# 2.2 Clients Disassociation Threshold

### Additions to the Setup menu

**Clients-Disassociation-Threshold**
A hanging rate adaption leads to a permanent communication interruption between an Access Point and 1 or more Clients. This command allows the user to automatically disassociate all Clients if the rate adaption on the Access Point hangs.

**WARNING**

**NON-FUNCTIONAL WIRELESS NETWORK**

Using this command with wrong settings can lead to a non-functional wireless network.
Therefore test the setting for this command before using it in production.

**Failure to follow this instruction can result in death, serious injury, or equipment damage.**

This command takes effect only on an 11 ac Access Point.

**SNMP ID:**

2.12.258

**Telnet path:**

**Setup** > **WLAN > Clients-Disassociation-Threshold**

**Possible values:**

Max. 10 characters from
[0-9]
Unit is packets per second (pps)

**Default:**

0

**How to find the best setting for this command**
You find the best setting for this command doing the following steps in an iterative manner:

1) Find out maximum packets per second sent from Access Point to a Client.
2) Set the maximum packets per second from 1) with this command.
3) Test the sensitivity of the threshold and adjust it. The sensitivity depends on the sum of packets per second and the amount of Clients connected to the Access Point because this is the load for the Access Point.

**Example 1:** The Access Point sends 20 packets per seconds to a Client (20 pps = maximum pps in our example). So let's set 20 as threshold:

*set /Setup/WLAN/Clients-Disassociation-Threshold 20*

What does this mean? It means that the Access Point sends 20 packets per second to the Client. If the Client does not respond to those packets with an acknowledge message, the Access Point will disassociate all Clients to resolve the hang of the rate adaption on the Access Point.

If the threshold is not sensitive enough, the threshold has to be reduced.
If the threshold is too sensitive, the threshold has to be increased.

**Example 2:** Disable this functionality.

*set /Setup/WLAN/Clients-Disassociation-Threshold 0*

# 2.3 Tx Timeouts

### Additions to the Setup menu

**Tx-Timeouts**
Too many Tx Timeouts lead to a permanent communication interruption between an Access Point and 1 or more Clients. This command allows the user to set a threshold after which the WLAN module is reset.

**WARNING**

**NON-FUNCTIONAL WIRELESS NETWORK**

Using this command with wrong settings can lead to a non-functional wireless network.
Therefore test the setting for this command before using it in production.

**Failure to follow this instruction can result in death, serious injury, or equipment damage.**

This command takes effect only on 11 ac devices.

**SNMP ID:**

2.12.259

**Telnet path:**

**Setup** > **WLAN** > **Tx-Timeouts**

**Possible values:**

Max. 10 characters
from [0-9]

**Default:**

0

**Example 1:** The device accepts 20 Tx Timeouts. So let's set 20 as threshold:

*set /Setup/WLAN/Tx-Timeouts 20*

What does this mean? It means that the WLAN module is reset if there are more than 20 Tx Timeouts.

If the threshold is not sensitive enough, the threshold has to be reduced.
If the threshold is too sensitive, the threshold has to be increased.

**Example 2:** Disable this functionality.

*set /Setup/WLAN/Tx-Timeouts 0*

HIRSCHMANN
A BELDEN BRAND

# Addendum
# HiLCOS Rel. 10.32

# 1 Addendum to HiLCOS Rel. 10.32

This document describes the changes and enhancements in HiLCOS Rel. 10.32 since the previous version.

# 2 Configuration

## 2.1 Configuration software

### 2.1.1 Automatic redirection of WEBconfig access to HTTPS

#### Additions to the Setup menu

**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.

**SNMP ID:**

2.21.24

**Telnet 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

## 2.1.2 WEBconfig with TLS 1.3

As of HiLCOS 10.32 your device supports TLS 1.3 for accessing WEBconfig. TLS 1.3 represents the latest advancement of the TLS standard and offers, for example, the exclusive use of state-of-the-art cipher suites and Perfect Forward Secrecy to provide improved security compared to previous versions.

An HiLCOS update automatically supplements the configuration with TLS 1.3 support for WEBconfig. If necessary, remove older methods that should no longer be available for WEBconfig.

### Additions to the Setup menu

#### Versions

This bitmask specifies which versions of the protocol are allowed.

**SNMP ID:**

2.21.40.3

**Telnet path:**

**Setup** > **HTTP** > **SSL**

**Possible values:**

**SSLv3**
**TLSv1**
**TLSv1.1**
**TLSv1.2**
**TLSv1.3**

**Default:**

TLSv1.2

TLSv1.3

# 3 Routing and WAN connections

## 3.1 Advanced Routing and Forwarding (ARF)

### 3.1.1 Routing tags for DNS forwarding

#### Additions to the Setup menu

**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.

**SNMP ID:**

2.17.17

**Telnet path:**

**Setup** > **DNS**

**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.

**SNMP ID:**

2.17.17.1

**Telnet path:**

**Setup** > **DNS** > **Loopback-Addresses**

**Possible values:**

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

**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.

**SNMP ID:**

2.17.17.2

**Telnet path:**

**Setup** > **DNS** > **Loopback-Addresses**

**Possible values:**

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

# 3.2 Locator / ID Separation Protocol (LISP)

## Additions to the Setup menu

### LISP

Settings for Locator / ID Separation Protocol (LISP).

**SNMP ID:**

2.93.4

**Telnet path:**

**Setup** > **Routing-Protocols**

**Instances**

This table contains the global configuration of the LISP instances on the device.

**SNMP ID:**

2.93.4.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Name**

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

**SNMP ID:**

2.93.4.1.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Operating**

Activates or deactivates this LISP instance.

**SNMP ID:**

2.93.4.1.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

**No**
**Yes**

**EID-Rtg-Tag**

Routing tag of the endpoint identifier (EID) of this instance.

**SNMP ID:**

2.93.4.1.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

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

**RLOC-Rtg-Tag**

Routing tag of the routing locator (RLOC) of this instance.

**SNMP ID:**

2.93.4.1.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

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

**Instance-ID**

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

**SNMP ID:**

2.93.4.1.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

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

**Probing-Method**

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries.

**SNMP ID:**

2.93.4.1.6

**Telnet 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.

**IPv6**

Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

**SNMP ID:**

2.93.4.1.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

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

**Default:**

600

**Admin-Distance**

Administrative routing distance.

**SNMP ID:**

2.93.4.1.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Instances**

**Possible values:**

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

**Default:**

240

**EID-Mapping**

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.

**SNMP ID:**

2.93.4.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Name**

References the name of the LISP instance.

**SNMP ID:**

2.93.4.2.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

### EID-Address-Type

This bitmask specifies the protocol version of the EID prefix when referencing the EID prefix via an interface or network name.

**SNMP ID:**

2.93.4.2.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

**IPv4**
**IPv6**

### 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.

**SNMP ID:**

2.93.4.2.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

Max. 43 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

### Locator-Address-Type

This bitmask specifies the protocol version of the RLOC when referencing the EID prefix via an interface name.

**SNMP ID:**

2.93.4.2.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

**IPv4**
**IPv6**

**Locator**

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

**SNMP ID:**

2.93.4.2.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Operating**

**SNMP ID:**

2.93.4.2.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

**No**
**Yes**

**Priority**

The priority of the EID mapping.

**SNMP ID:**

2.93.4.2.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

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

**Default:**

1

**Weight**

The weight of the EID mapping.

**SNMP ID:**

2.93.4.2.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

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

**Default:**

100

**Comment**

Enter a descriptive comment for this entry.

**SNMP ID:**

2.93.4.2.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

Max. 25 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**ITR-Settings**

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).

**SNMP ID:**

2.93.4.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Name**

References the name of the LISP instance.

**SNMP ID:**

2.93.4.3.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Map-Resolver**

IPv4 or IPv6 address of the LISP map resolver.

**SNMP ID:**

2.93.4.3.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

**Operating**

Activates or deactivates these ITR settings.

**SNMP ID:**

2.93.4.3.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

**No**
**Yes**

**Loopback address**

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

**SNMP ID:**

2.93.4.3.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

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

**Rtg-Tag**

Routing tag used to access the map resolver.

**SNMP ID:**

2.93.4.3.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

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

**Map-Resolver-Retries**

Number of retries for map requests to the map resolver.

**SNMP ID:**

2.93.4.3.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

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

**Default:**

3

**Map-Request-Route-IPv4**

Specifies the IPv4 route or prefix for the LISP map requests.

**SNMP ID:**

2.93.4.3.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

Max. 18 characters from `[A-F][a-f][0-9]:.`

**Map-Request-Route-IPv6**

Specifies the IPv6 route or prefix for the LISP map requests.

**SNMP ID:**

2.93.4.3.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ITR-Settings**

**Possible values:**

Max. 43 characters from `[A-F][a-f][0-9]:.`

**ETR-Settings**

This table specifies the parameters for the role as Egress Tunnel Router (ETR).

**SNMP ID:**

2.93.4.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Name**

References the name of the LISP instance.

**SNMP ID:**

2.93.4.4.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Map-Server**

IPv4 or IPv6 address of the LISP map server

**SNMP ID:**

2.93.4.4.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

**Operating**

Activates or deactivates these ETR settings.

**SNMP ID:**

2.93.4.4.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

**No**
**Yes**

**Loopback address**

Contains the sender address as the named interface that is used with the map server in LISP communication.

**SNMP ID:**

2.93.4.4.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

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

**Rtg-Tag**

Routing tag to be used to access the map server.

**SNMP ID:**

2.93.4.4.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

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

**Map-Cache-TTL-Minutes**

Time-to-live of the EID mappings in minutes registered with the map server.

**SNMP ID:**

2.93.4.4.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

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

**Map-Register-Interval-Seconds**

Registration interval in seconds in which map registrations are sent to the map server.

**SNMP ID:**

2.93.4.4.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

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

**Key-Type**

Algorithm used for authentication at the map server.

**SNMP ID:**

2.93.4.4.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

**None**
**HMAC-SHA-1-96**
**HMAC-SHA-256-128**

**Key**

Key or password used to register the EID mapping on the map server.

**SNMP ID:**

2.93.4.4.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

Max. 24 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

### 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.

**SNMP ID:**

2.93.4.4.10

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

**No**
**Yes**

### 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.

**SNMP ID:**

2.93.4.4.11

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **ETR-Settings**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

### Operating

This item switches the routing protocol Locator / ID Separation Protocol (LISP) on or off.

**SNMP ID:**

2.93.4.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.93.4.7

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.93.4.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Possible values:**

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

**Default:**

0

### Native-Forward

**SNMP ID:**

2.93.4.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

### Name

References the name of the LISP instance.

**SNMP ID:**

2.93.4.9.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Native-Forward**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

### Type

**SNMP ID:**

2.93.4.9.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Native-Forward**

**Possible values:**

**None**
**ProxyXTR**
**Interface**

### Proxy-XTR

**SNMP ID:**

2.93.4.9.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Native-Forward**

**Possible values:**

Max. 43 characters from `[A-F][a-f][0-9]:.`

**Interface**

**SNMP ID:**

2.93.4.9.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Native-Forward**

**Possible values:**

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

**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.

**SNMP ID:**

2.93.4.10

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP**

**Name**

References the name of the LISP instance.

**SNMP ID:**

2.93.4.10.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Redistribution**

**Possible values:**

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Source**

This bitmask specifies the route sources of the imported routes.

**SNMP ID:**

2.93.4.10.2

**Telnet 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.

**Destination**

Specifies the destination of routes imported to LISP.

**SNMP ID:**

2.93.4.10.3

**Telnet 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.

**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.

**SNMP ID:**

2.93.4.10.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Redistribution**

**Possible values:**

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Priority**

The priority.

**SNMP ID:**

2.93.4.10.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **Redistribution**

**Possible values:**

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

**Default:**

1

**Weight**

The weight of the EID mapping.

**SNMP ID:**

2.93.4.2.8

**Telnet path:**

**Setup** > **Routing-Protocols** > **LISP** > **EID-Mapping**

**Possible values:**

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

**Default:**

100

# 3.3 Route redistribution of LISP and RIP routes in BGP

As of HiLCOS 10.32, route redistribution allows LISP and RIP routes be redistributed according to BGP. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by BGP.

The redistribution of RIP routes is only supported for IPv4 routes.

## Additions to the Setup menu

### 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).

**SNMP ID:**

2.93.1.4.1.9

**Telnet 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.

### 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).

**SNMP ID:**

2.93.1.4.2.9

**Telnet 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.

# 3.4 BGP: Setting administrative distance by policy

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.93.1.5.2.1.9

**Telnet path:**

**Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

**Possible values:**

Max. 3 characters from `[0–9]`

# 3.5 Filter list for redistribution in BGP

## Additions to the Setup menu

### Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

**SNMP ID:**

2.93.1.4.1.11

**Telnet path:**

**Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

**Possible values:**

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

**Default:**

*empty*

### Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

**SNMP ID:**

2.93.1.4.1.12

**Telnet path:**

**Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

**Possible values:**

**Allow**
**Reject**

**Default:**

Allow

### Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

**SNMP ID:**

2.93.1.4.2.11

**Telnet path:**

**Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

**Possible values:**

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

**Default:**

*empty*

## Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

**SNMP ID:**

2.93.1.4.2.12

**Telnet path:**

**Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

**Possible values:**

**Allow**
**Reject**

**Default:**

Allow

## Filter

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP.

**SNMP ID:**

2.93.5

**Telnet path:**

**Setup** > **Routing-Protocols**

**Prefix-List**

Here you specify a prefix list that can be referenced by BGP.

**SNMP ID:**

2.93.5.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter**

**Name**

Contains the name of this entry.

**SNMP ID:**

2.93.5.1.1

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

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

**Default:**

*empty*

**IP-Address**

Contains the IPv4 or IPv6 address of the network.

**SNMP ID:**

2.93.5.1.2

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

Max. 39 characters from `[A-F][a-f][0-9]:.`

**Default:**

*empty*

**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**.

**SNMP ID:**

2.93.5.1.3

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

*empty*

**Length-Min**

Specifies the minimum prefix length value required for the prefix to match.

**SNMP ID:**

2.93.5.1.4

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

*empty*

**Length-Max**

Specifies the maximum prefix length value required for the prefix to match.

**SNMP ID:**

2.93.5.1.5

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

*empty*

**Comment**

Comment on this entry.

**SNMP ID:**

2.93.5.1.6

**Telnet path:**

**Setup** > **Routing-Protocols** > **Filter** > **Prefix-List**

**Possible values:**

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

**Default:**

*empty*

# 3.6 BGP: Switch for default route propagation

As of Addendum HiLCOS Rel. 10.32 your device has the option to handle default routes like normal routes with BGP.

## Additions to the Setup menu

### Send-Default-Route

This switch determines the behavior of the propagation of default routes.

**SNMP ID:**

2.93.1.3.11

**Telnet 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* or *2.93.1.6.2 IPv6*).

**Default:**

No

# 4 IPv6

## 4.1 IPv6 WAN interface

### Additions to the Setup menu

#### IPv6

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

**SNMP ID:**

2.2.2.8

**Telnet path:**

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

**Possible values:**

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

**Default:**

DEFAULT

#### IPv6

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

**SNMP ID:**

2.2.19.19

**Telnet path:**

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

**Possible values:**

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

**Default:**

DEFAULT

### IPv6

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

**SNMP ID:**

2.2.21.9

**Telnet path:**

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

**Possible values:**

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

**Default:**

DEFAULT

### IPv6

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

**SNMP ID:**

2.2.37.5

**Telnet path:**

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

**Possible values:**

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

**Default:**

DEFAULT

### IPv6

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

**SNMP ID:**

2.2.51.11

**Telnet path:**

**Setup** > **WAN** > **GRE-Tunnel**

**Possible values:**

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

**Default:**

DEFAULT

## IPv6

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

**SNMP ID:**

2.19.9.20

**Telnet path:**

**Setup** > **VPN** > **VPN-Peers**

**Possible values:**

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

**Default:**

DEFAULT

## IPv6

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

**SNMP ID:**

2.19.36.1.21

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

**Default:**

DEFAULT

## Interface name

Give a name to the device IPv6 WAN interface here. This name is specified at the remote site. 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.

**SNMP ID:**

2.70.7.1

**Telnet path:**

**Setup** > **IPv6** > **WAN-Interfaces**

**Possible values:**

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

**Default:**

DEFAULT

# 4.2 DHCPv6

## Additions to the Setup menu

### 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

**SNMP ID:**

2.70.3.1.6.3

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

A hex string with max. 127 characters `[a-z][0-9]:-`

**Default:**

*empty*

### Identifier-Type

This type specifies how the identifier in 2.70.3.1.6.3 is to be interpreted.

**SNMP ID:**

2.70.3.1.6.8

**Telnet 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.

**Comment**

Enter a descriptive comment for this entry.

**SNMP ID:**

2.70.3.1.6.9

**Telnet path:**

**Setup** > **IPv6** > **DHCPv6** > **Server** > **Reservations**

**Possible values:**

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

**Default:**

*empty*

# 5 Firewall

## 5.1 SD-WAN application routing / Layer-7 application control

### Additions to the Setup menu

#### 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

**SNMP ID:**

2.70.5.25

**Telnet path:**

**Setup** > **IPv6** > **Firewall**

**Possible values:**

**No**
**Yes**

**Default:**

No

## Firewall

Firewall settings

**SNMP ID:**

2.110

**Telnet path:**

**Setup**

**DNS-Destinations**

As of HiLCOS 10.32 DNS names can be used in the firewall. DNS names can be defined in full, e.g. "www.hirschmann.de", or as a wildcard expression, e.g. "*hirschmann*". These objects can be used in firewall rules as destinations. Layer-7 (web) applications can be blocked, allowed, limited, prioritized, or redirected to another routing context.
Further information and recommendations are available in the Reference Manual under the Firewall section.

**SNMP ID:**

2.110.1

**Telnet path:**

**Setup** > **Firewall**

**Name**

The name for this DNS destination. This name is used to reference this object.

**SNMP ID:**

2.110.1.1

**Telnet path:**

**Setup** > **Firewall** > **DNS-Destinations**

**Possible values:**

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

**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. "*.hirschmann.*". 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.

**SNMP ID:**

2.110.1.2

**Telnet path:**

**Setup** > **Firewall** > **DNS-Destinations**

**Possible values:**

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**DNS-Destination-List**

In the DNS destination list, you can group multiple DNS destinations into one referenced object.

**SNMP ID:**

2.110.2

**Telnet path:**

**Setup** > **Firewall**

**Name**

The name for this DNS destination list. This name is used to reference this object.

**SNMP ID:**

2.110.2.1

**Telnet path:**

**Setup** > **Firewall** > **DNS-Destination-List**

**Possible values:**

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

**Targets**

Contains a comma-separated or space-separated list of names of the DNS destinations.

**SNMP ID:**

2.110.2.2

**Telnet path:**

**Setup** > **Firewall** > **DNS-Destination-List**

**Possible values:**

Max. 252 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

**Default:**

*empty*

# 6 Wireless LAN – WLAN

## 6.1 WPA3 (Wi-Fi Protected Access 3)

### Additions to the Setup menu

#### WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

**SNMP ID:**

2.23.20.3.9

**Telnet path:**

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

**Possible values:**

**WPA1**
**WPA2**
**WPA1/2**
**WPA2/3**
**WPA3**
**WPA1/2/3**

**Default:**

WPA2

## SAE-Groups

The authentication method SAE (Simultaneous Authentication of Equals) uses elliptic curves. Further information is available from the *Standards for Efficient Cryptography Group*.

**SNMP ID:**

2.23.20.3.26

**Telnet path:**

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

**Possible values:**

**secp256r1**
**secp384r1**
**secp521r1**
**secp192r1**
**secp224r1**

**Default:**

secp256r1

secp384r1

secp521r1

## WPA2-3-Session-Keytypes

From Addendum HiLCOS Rel. 10.32 this setting replaces the value 2.23.20.3.13 **WPA2-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.

**SNMP ID:**

2.23.20.3.27

**Telnet path:**

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

**Possible values:**

**AES-CCMP-128**
**AES-CCMP-256**
**AES-GCMP-128**
**AES-GCMP-256**

**Default:**

AES-CCMP-128

## 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!

**SNMP ID:**

2.23.20.3.28

**Telnet 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

# 6.2 Enhanced Open

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.3.4

**Telnet 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

### Enhanced-Open-Groups

The authentication method Enhanced Open uses elliptic curves.

**SNMP ID:**

2.23.20.3.22

**Telnet path:**

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

**Possible values:**

**secp256r1**
**secp384r1**
**secp521r1**

**Default:**

secp256r1

secp384r1

secp521r1

# 6.3 Enhanced Passphrase Security (LEPS)

## Additions to the Setup menu

### LEPS-U

Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

**SNMP ID:**

2.12.133

**Telnet path:**

**Setup** > **WLAN**

**Operating**

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

**SNMP ID:**

2.12.133.1

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U**

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.12.133.2

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U**

**Name**

Enter a unique name for the LEPS-U profile here.

**SNMP ID:**

2.12.133.2.1

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Profiles**

**Possible values:**

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

**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.

**SNMP ID:**

2.12.133.2.2

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Per-Client-Tx-Limit**

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

**SNMP ID:**

2.12.133.2.3

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Special values:**

**0**

No limit.

**Per-Client-Rx-Limit**

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

**SNMP ID:**

2.12.133.2.4

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Special values:**

**0**

No limit.

**VLAN-ID**

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

**SNMP ID:**

2.12.133.2.5

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Users**

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

**SNMP ID:**

2.12.133.3

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U**

**Name**

Enter a unique name for the LEPS-U user here.

**SNMP ID:**

2.12.133.3.1

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

**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.

**SNMP ID:**

2.12.133.3.2

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

**WPA passphrase**

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

**SNMP ID:**

2.12.133.3.3

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

**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.

**SNMP ID:**

2.12.133.3.4

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

**Special values:**

**0**

No limit.

**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.

**SNMP ID:**

2.12.133.3.5

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

**Special values:**

**0**

No limit.

**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.

**SNMP ID:**

2.12.133.3.6

**Telnet path:**

**Setup** > **WLAN** > **LEPS-U** > **Users**

**Possible values:**

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

## LEPS-U

Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

**SNMP ID:**

2.37.1.25

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration**

**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.

**SNMP ID:**

2.37.1.25.1

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

**Name**

Enter a unique name for the LEPS-U profile here.

**SNMP ID:**

2.37.1.25.1.1

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

**Possible values:**

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

**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.

**SNMP ID:**

2.37.1.25.1.2

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Per-Client-Tx-Limit**

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

**SNMP ID:**

2.37.1.25.1.3

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

**Possible values:**

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

**Special values:**

**0**

No limit.

**Per-Client-Rx-Limit**

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

**SNMP ID:**

2.37.1.25.1.4

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

**Possible values:**

Max. 9 characters from `[0–9]`

**Special values:**

**0**

No limit.

**VLAN-ID**

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

**SNMP ID:**

2.37.1.25.1.5

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

**Possible values:**

Max. 4 characters from `[0–9]`

**Users**

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

**SNMP ID:**

2.37.1.25.2

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

**Name**

Enter a unique name for the LEPS-U user here.

**SNMP ID:**

2.37.1.25.2.1

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

**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.

**SNMP ID:**

2.37.1.25.2.2

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

**WPA passphrase**

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

**SNMP ID:**

2.37.1.25.2.3

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

**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.

**SNMP ID:**

2.37.1.25.2.4

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

**Special values:**

**0**

No limit.

**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.

**SNMP ID:**

2.37.1.25.2.5

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

**Special values:**

**0**

No limit.

**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.

**SNMP ID:**

2.37.1.25.2.6

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

**Possible values:**

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

# 6.4 Client Management

## Additions to the Setup menu

### Band 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.

**SNMP ID:**

2.12.87

**Telnet path:**

**Setup** > **WLAN**

**Operating**

This option enables WLAN Band Steering or Client Management in the access point.

**SNMP ID:**

2.12.87.1

**Telnet path:**

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

**Dry-Run**

Client Management performs a test run. The scans are performed, decisions are calculated and logged, but not executed.

**SNMP ID:**

2.12.87.6

**Telnet path:**

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

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.12.87.7

**Telnet path:**

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

**Possible values:**

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

**Special values:**

**0**

This value disables the delay.

**Default:**

5

**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.

**SNMP ID:**

2.12.87.8

**Telnet path:**

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

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

5

**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.

**SNMP ID:**

2.12.87.9

**Telnet path:**

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

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

80

**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.

**SNMP ID:**

2.12.87.10

**Telnet path:**

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

**Possible values:**

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

**Default:**

10

**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.

**SNMP ID:**

2.12.87.11

**Telnet path:**

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

**Possible values:**

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

**Default:**

20

**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.

**SNMP ID:**

2.12.87.12

**Telnet path:**

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

**Possible values:**

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

**Default:**

-70

**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.

**SNMP ID:**

2.12.87.13

**Telnet path:**

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

**Possible values:**

**No**
**Yes**

**Default:**

No

**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.

**SNMP ID:**

2.12.87.14

**Telnet path:**

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

**Possible values:**

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

**Default:**

5

**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.

**SNMP ID:**

2.12.87.15

**Telnet path:**

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

**Possible values:**

0 … 23

**Default:**

3

**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.

**SNMP ID:**

2.12.87.16

**Telnet path:**

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

**Possible values:**

200 … 1000

**Default:**

400

**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.

**SNMP ID:**

2.12.87.17

**Telnet path:**

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

**Possible values:**

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

**Default:**

-75

**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.

**SNMP ID:**

2.12.87.18

**Telnet path:**

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

**Possible values:**

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

**Default:**

600

**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.

**SNMP ID:**

2.12.87.19

**Telnet path:**

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

**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:*`.

**SNMP ID:**

2.12.87.19.1

**Telnet path:**

**Setup** > **WLAN** > **Band-Steering** > **Blacklist-Clients**

**Possible values:**

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

**Default:**

*empty*

**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`.

**SNMP ID:**

2.12.87.20

**Telnet path:**

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

**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.

**SNMP ID:**

2.12.87.21

**Telnet path:**

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

**Possible values:**

**AP-Steering**
**AP+Band-Steering**

**Default:**

AP+Band-Steering

**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.

**SNMP ID:**

2.12.87.22

**Telnet path:**

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

**Possible values:**

Max. 3 characters from `[0–9]`

**Default:**

75

**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.

**SNMP ID:**

2.12.87.23

**Telnet path:**

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

**Possible values:**

Max. 4 characters from `–[0–9]`

**Default:**

-65

## Roaming-Targets

With Client Management enabled, the table under `/Status/WLAN/Roaming-Targets` is filled out automatically. The targets added manually to this table are also included into the list of neighbors by 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 87.

**SNMP ID:**

2.12.132

**Telnet path:**

**Setup** > **WLAN**

**Name**

Enter the name for the roaming target here.

**SNMP ID:**

2.12.132.1

**Telnet path:**

**Setup** > **WLAN** > **Roaming-Target**

**Possible values:**

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

# 6.5 Reduction of sensitivity for received packets

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.8.35

**Telnet path:**

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

**Possible values:**

0 … 20

## 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.

**SNMP ID:**

2.37.1.4.37

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-configuration** > **Accesspoints**

**Possible values:**

0 … 20

## 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.

**SNMP ID:**

2.37.1.4.38

**Telnet path:**

**Setup** > **WLAN-Management** > **AP-configuration** > **Accesspoints**

**Possible values:**

0 … 20

# 6.6 Separate switch to enable e-mail notification

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.12.41

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

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

**Default:**

*empty*

### Send-Mails

Determines whether notifications about WLAN events are sent to the e-mail address specified in 2.12.41 .

**SNMP ID:**

2.12.141

**Telnet path:**

**Setup** > **WLAN**

**Possible values:**

**No**
**Yes**

**Default:**

No

# 6.7 IEEE 802.11k Roaming Targets

## Additions to the Setup menu

### 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*.

**SNMP ID:**

2.12.132

**Telnet path:**

**Setup** > **WLAN**

**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.

**SNMP ID:**

2.12.132.1

**Telnet path:**

**Setup** > **WLAN** > **Roaming-Target**

**Possible values:**

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

# 6.8 Setting target EIRP

## Additions to the Setup menu

### Power-Setting

In versions before HiLCOS 10.32, 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 HiLCOS 10.32, 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.

**SNMP ID:**

2.23.20.8.33

**Telnet 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

### 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.

**SNMP ID:**

2.23.20.8.34

**Telnet path:**

**Setup** > **Interfaces** > **WLAN** > **Radio-settings**

**Possible values:**

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

# 7 WLAN management

## 7.1 New mode for antenna gain

### Additions to the Setup menu

#### 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. As of HiLCOS 10.32, there is a configuration option, that the standard antenna gain of a managed access point can be transmitted to the WLAN controller and is used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.32. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

**SNMP ID:**

2.37.1.4.35

**Telnet 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

## 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. As of HiLCOS 10.32, there is a configuration option, that the standard antenna gain of a managed access point can be transmitted to the WLAN controller and is used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.32. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

**SNMP ID:**

2.37.1.4.36

**Telnet 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

# 8 Virtual Private Networks – VPN

## 8.1 OCSP server

### Additions to the Setup menu

#### OCSP-AIA

When creating a certificate using Smart Certificate, the field "OCSP AIA" (OCSP Authority Information Access) can be displayed.

**SNMP ID:**

2.39.2.14.2.18

**Telnet 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

#### OCSP-AIA

Enter the name or IP address where OCSP clients can reach the OCSP server.

**SNMP ID:**

2.39.2.14.1.19

**Telnet path:**

**Setup** > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

**Possible values:**

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

**Default:**

*empty*

## OCSP server

This table contains the settings for the OCSP server.

**SNMP ID:**

2.39.7

**Telnet path:**

**Setup** > **Certificates**

### Operating

Turn the OCSP server on or off here.

**SNMP ID:**

2.39.7.1

**Telnet path:**

**Setup** > **Certificates** > **OCSP-Server**

**Possible values:**

**Yes**
**No**

**Default:**

No

### Port

The port used by the OCSP server.

**SNMP ID:**

2.39.7.2

**Telnet path:**

**Setup** > **Certificates** > **OCSP-Server**

**Possible values:**

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

**Default:**

8084

### 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=Hirschmann Automation and Control GmbH/C=DE
```

In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

**SNMP ID:**

2.39.7.3

**Telnet path:**

**Setup** > **Certificates** > **OCSP-Server**

**Possible values:**

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

**Default:**

/CN=ocspresponder.example.test/O=Hirschmann Automation and Control GmbH/C=DE

**WAN access**

This setting determines if and how the OCSP server can be reached from the WAN.

**SNMP ID:**

2.39.7.4

**Telnet path:**

**Setup** > **Certificates** > **OCSP-Server**

**Possible values:**

**Yes**
**No**
**Over-VPN**

**Default:**

No

**Signature-Algo**

The algorithm used to generate the certificate used by the OCSP server.

**SNMP ID:**

2.39.7.5

**Telnet path:**

**Setup** > **Certificates** > **OCSP-Server**

**Possible values:**

**SHA1**
**SHA-256**
**SHA-384**
**SHA-512**

**Default:**

SHA-256

# 8.2 Layer-3 Ethernet tunnel with Layer-2 Tunneling Protocol version 3 (L2TPv3)

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.2.35.11

**Telnet path:**

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

**Possible values:**

**L2TPv2**

Layer 2 Tunneling Protocol Version 2

**L2TPv3**

Layer 2 Tunneling Protocol Version 3

### Operating

This L2TP endpoint is enabled or disabled.

**SNMP ID:**

2.2.35.12

**Telnet path:**

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

**Possible values:**

**No**

L2TP endpoint is disabled.

**Yes**

L2TP endpoint is enabled.

## 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.

**SNMP ID:**

2.2.39

**Telnet path:**

**Setup** > **WAN**

#### 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.

**SNMP ID:**

2.2.39.1

**Telnet path:**

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

**Possible values:**

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

#### 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.

**SNMP ID:**

2.2.39.2

**Telnet path:**

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

**Possible values:**

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

**Interface**

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

**SNMP ID:**

2.2.39.3

**Telnet path:**

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

**Possible values:**

**L2TP-ETHERNET-1 … L2TP-ETHERNET-16**

16 virtual L2TP Ethernet interfaces

# 8.3 IKEv2

**Additions to the Setup menu**

**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.

**SNMP ID:**

2.19.36.3.4.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

**Possible values:**

**RSASSA-PSS**
**RSASSA-PKCS1-v1_5**

**Default:**

RSASSA-PSS

**Additions to the Setup menu**

**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 Hirschmann 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.

**SNMP ID:**

2.19.36.4.7

**Telnet 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

**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.

**SNMP ID:**

2.19.36.4.8

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **General**

**Possible values:**

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

**Default:**

0

### 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**.

**SNMP ID:**

2.19.36.1.22

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **Peers**

**Possible values:**

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

## Local-Auth

Sets the authentication method for the local identity.

**SNMP ID:**

2.19.36.3.1.2

**Telnet 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

## Remote-Auth

Sets the authentication method for the remote identity.

**SNMP ID:**

2.19.36.3.1.6

**Telnet 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

## Remote-Auth

Sets the authentication method for the remote identity.

**SNMP ID:**

2.19.36.3.3.2

**Telnet 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

## 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

**SNMP ID:**

2.19.36.7.2.6

### Telnet path:

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

**Possible values:**

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

**Default:**

*empty*

## 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 Hirschmann 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.

**SNMP ID:**

2.19.36.7.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG**

**Domain-Lists**

Here you specify the domain lists for split DNS.

**SNMP ID:**

2.19.36.7.3.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

**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.

**SNMP ID:**

2.19.36.7.3.1.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

**Possible values:**

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

**Default:**

*empty*

**Domain-List**

Enter a name for the domain lists.

**SNMP ID:**

2.19.36.7.3.1.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

**Possible values:**

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

**Default:**

*empty*

**Profiles**

Here you set the profiles for split DNS.

**SNMP ID:**

2.19.36.7.3.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

**Name**

Enter a name for this profile.

**SNMP ID:**

2.19.36.7.3.4.1

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

**Possible values:**

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

**Default:**

*empty*

**Send-DNS-Forwardings**

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

**SNMP ID:**

2.19.36.7.3.4.2

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Send-local-Domain**

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

**SNMP ID:**

2.19.36.7.3.4.3

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

**Possible values:**

**No**
**Yes**

**Default:**

No

**Domain-List**

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

**SNMP ID:**

2.19.36.7.3.4.4

**Telnet path:**

**Setup** > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

**Possible values:**

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

**Default:**

*empty*

## 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. Hirschmann VPN routers at both ends must have at least HiLCOS 10.32.

**SNMP ID:**

2.19.36.12

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Possible values:**

**Off**
**Always**

**Default:**

Off

## 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.

**SNMP ID:**

2.19.36.14

**Telnet path:**

**Setup** > **VPN** > **IKEv2**

**Possible values:**

**No**
Password rules enforcement is disabled.

**Yes**
Password rules enforcement is enabled.

**Default:**

No

## RSA-Padding-Method

Specifies the RSA padding method for certificates issued by the SCEP-CA.

**SNMP ID:**

2.39.2.15

**Telnet 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

# 9 RADIUS

## 9.1 User-defined attributes for RADIUS users in the RADIUS server

### Additions to the Setup menu

#### Attribute-Values

User-defined attributes for RADIUS users in the RADIUS server.

Along with the user-management attributes supported by the Hirschmann RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users here.

**SNMP ID:**

2.25.10.7.25

**Telnet path:**

**Setup** > **RADIUS** > **Server** > **Users**

**Possible values:**

Comma-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*

# 10 Other services

## 10.1 Automatic IP address administration with DHCP

### 10.1.1 Configuring DHCPv4 parameters with LANconfig

#### Additions to the Setup menu

**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.

**SNMP ID:**

2.10.20.22

**Telnet path:**

**Setup** > **DHCP**

**Possible values:**

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

**Default:**

*empty*

#### DHCP options

#### Additions to the Setup menu

**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.

**SNMP ID:**

2.10.26.5

**Telnet path:**

**Setup** > **DHCP** > **Additional-Options**

**Possible values:**

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

**Default:**

*empty*

**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 Hirschmann devices always contain the string "Hirschmann" 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.

**SNMP ID:**

2.10.26.6

**Telnet path:**

**Setup** > **DHCP** > **Additional-Options**

**Possible values:**

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

**Default:**

*empty*

**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.

**SNMP ID:**

2.10.26.7

**Telnet path:**

**Setup** > **DHCP** > **Additional-Options**

**Possible values:**

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

**Default:**

*empty*

## Assigning IP addresses based on DHCP option 82

### Additions to the Setup menu

#### 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.

**SNMP ID:**

2.10.27

**Telnet path:**

**Setup** > **DHCP**

## Circuit-ID

**SNMP ID:**

2.10.27.1

**Telnet path:**

**Setup** > **DHCP** > **Relay-Info-List**

**Possible values:**

Max. 64 characters from `[A-F][a-f]x[0-9]{}/`

## 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.

**SNMP ID:**

2.10.27.2

**Telnet path:**

**Setup** > **DHCP** > **Relay-Info-List**

## 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.

**SNMP ID:**

2.10.27.3

**Telnet path:**

**Setup** > **DHCP** > **Relay-Info-List**

**Possible values:**

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

**Default:**

*empty*

## 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.

**SNMP ID:**

2.10.27.4

**Telnet path:**

**Setup** > **DHCP** > **Relay-Info-List**

**Possible values:**

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

**Default:**

*empty*

# 10.2 DHCP server – suppress ARP request

As of HiLCOS Rel. 10.32 your device supports the option to suppress the ARP request that usually precedes the assignment of an IP address.

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.10.20.23

**Telnet path:**

**Setup** > **DHCP** > **Network-List**

**Possible values:**

**Yes**

Do not carry out check by ARP request.

**No**

Perform check by ARP request.

**Default:**

No

# 10.3 Simple Network Management Protocol (SNMP)

## Additions to the Setup menu

### 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**.

**SNMP ID:**

2.11.93

**Telnet path:**

**Setup** > **Config**

**Possible values:**

**No**

Password rules enforcement is disabled.

**Yes**

Password rules enforcement is enabled.

**Default:**

No

# 10.4 TACACS+

## 11.4.1 Configuring the TACACS+ server

### Additions to the Setup menu

**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.

**SNMP ID:**

2.54.9.1

**Telnet path:**

**Setup** > **Tacacs+** > **Server**

**Possible values:**

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

**Default:**

*empty*

# 11 Quality of Service

## 11.1 Configurable DSCP tags for internal Hirschmann services

### Additions to the Setup menu

#### DSCP marking

Internal HiLCOS 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.

**SNMP ID:**

2.11.94

**Telnet path:**

**Setup** > **Config**

**Application**

Column with the internal applications.

**SNMP ID:**

2.11.94.1

**Telnet path:**

**Setup** > **Config** > **DSCP-Marking**

**DSCP**

Column with the DiffServ codepoints. Default values are listed for the possible internal applications.

**SNMP ID:**

2.11.94.2

**Telnet 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

HIRSCHMANN
A BELDEN BRAND

# Addendum
# HiLCOS Rel. 10.34

# Addendum to HiLCOS Rel. 10.34

This document describes the changes and enhancements in HiLCOS Rel. 10.34 since the previous release.

# 1 Voice over IP – VoIP

## 1.1 Dynamic SIP lines

### Additions to the Setup menu

#### Dynamic line

Configure the dynamic SIP lines here.

**SNMP ID:**

2.33.4.1.

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Line** > **SIP-Provider**

**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.

**SNMP ID:**

2.33.4.1.3.1

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

**Possible values:**

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

**SIP line name**

Here you specify one of the already configured physical SIP connections.

**SNMP ID:**

2.33.4.1.3.2

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

**Possible values:**

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

**Priority**

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

**SNMP ID:**

2.33.4.1.3.3

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

**Possible values:**

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

**Weight**

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

**SNMP ID:**

2.33.4.1.3.4

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

**Possible values:**

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

**Algorithm**

The algorithm must be configured identically for all entries that belong to a dynamic line.

**SNMP ID:**

2.33.4.1.3.5

**Telnet 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.

**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.

**SNMP ID:**

2.33.4.1.3.6

**Telnet path:**

**Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

**Possible values:**

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

# 1.2 Flex mode

## Additions to the Setup menu

### 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".

**SNMP ID:**

2.33.4.1.1.17

**Telnet 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 TCP-IP Alive-Test

## Additions to the Setup menu

### Loopback-Address

Here you assign a loopback address (name of an ARF network, named loopback address or IP address) to be used for the alive test.

**SNMP ID:**

2.7.21.8

**Telnet path:**

**Setup > TCP-IP > Alive-Test**

**Possible values:**

**Valid IP address**

**Default:**

0.0.0.0

### Time-Unit

As of HiLCOS 10.34, this feature operates not only in seconds but also in milliseconds. The support of milliseconds provides higher granularity for the Mesh Network feature. The user is now able to change the scale of the alive test timeout values from seconds to milliseconds and vice versa.

**SNMP ID:**

2.7.21.248

**Telnet path:**

**Setup > TCP-IP > Alive-Test**

**Possible values:**

**Seconds**
**Milliseconds**

**Default:**

Seconds

# 3 WLAN

## 3.1 Mesh Network

### Additions to the Setup menu

#### Mesh-Network

The WLAN mesh solution establishes an automatic configuration of the links between the wireless network's nodes. It simplifies and accelerates the network installation process in a new location. With its link detection mechanism, the connectivity with the root node can be monitored. Reconfiguration mechanisms help reduce downtime when an existing connection is terminated. This solution assumes that the wireless network will be connected to the back-haul using wired infrastructure. It will be implemented for BAT devices that have 2 radio modules. One radio module interface (WLAN-2) is configured to operate in station mode, the other WLAN interface (WLAN-1) is configured to operate in access point mode. The access point interface provides the next backhaul (mesh) network SSID and access network SSIDs. It uses the existing alive test feature to monitor the connection.

**SNMP ID:**

2.12.252

**Telnet path:**

**Setup > WLAN**

#### Mesh-Interface

This interface allows the user to select the logical interface that will connect the next node into the mesh network.

**SNMP ID:**

2.12.252.1

**Telnet path:**

**Setup** > **WLAN** > **Mesh-Network**

**Possible values:**

**WLAN-1**
**WLAN-1-2**
**WLAN-1-3**
**WLAN-1-4**
**WLAN-1-5**
**WLAN-1-6**
**WLAN-1-7**
**WLAN-1-8**

**Default:**

WLAN-1

**Access-Interface**
This interface allows the user to select the logical interface with which data for different purposes can be collected.

**SNMP ID:**

2.12.252.2

**Telnet path:**

**Setup** > **WLAN** > **Mesh-Network**

**Possible values:**

**WLAN-1**
**WLAN-1-2**
**WLAN-1-3**
**WLAN-1-4**
**WLAN-1-5**
**WLAN-1-6**
**WLAN-1-7**
**WLAN-1-8**

**Default:**

WLAN-1-2

## 3.2 Selection Preference Access Point Station

### Additions to the Setup menu

#### Selection-Preference-AP-Station

This feature allows to select the access point that has the least number of stations connected to it.

**SNMP ID:** 2.12.254

**Telnet path:** **Setup > WLAN**

**Possible values:**

No - Access point with the lowest channel utilization will be selected.
- If 2 or more access points habe the same lowest channel utilization, the access point with the highest signal strength will be selected.

Yes - Access point with the least number of connected stations will be selected.
- If 2 or more access points habe the same number of connected stations, the access point with the lowest channel utilization will be selected.
- If the above parameters are the same, the access point with the highest signal strength will be selected.

**Default:** Yes

## 3.3 Endless Scan Fix (Applies only to BAT867 devices)

Two features have been added: One for setting the packet receive timeout (Restart-On-Pkt-Recv-Timeout), and the other for defining the maximum number of rescans (Restart-Chk-On-Unsuccessful-Scan-Cnt) . Upon packet receive timeout expiry, if the specified number of rescans has been exceeded without receiving packets, the WLAN card is considered to be in a hang state and is restarted. For this reason, both features must be configured. By default, both features are disabled.

### Additions to the Setup menu

#### Restart-On-Pkt-Recv-Timeout

This feature allows to set the packet receive timeout.

**SNMP ID:** 2.12.258

**Telnet path:** **Setup > WLAN**

**Possible values:** 0 to 2147483647milliseconds

**Default:** 0 (disabled)

#### Restart-Chk-On-Unsuccessful-Scan-Cnt

This feature allows to set the the maximum number of rescans.

**SNMP ID:** 2.12.259

**Telnet path:** **Setup > WLAN**

**Possible values:** 0 to 255

**Default:** 0 (disabled)

# 4 Network

## Additions to the Setup menu

### 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.

**SNMP ID:**

2.23.20.1.25

**Telnet path:**

**Setup > Interfaces > WLAN > Network**

**Possible values:**

Max. 10 characters from `0123456789`

**Default:**

0

**Special values:**

**0**

Disables the limit.

### 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.

**SNMP ID:**

2.23.20.1.26

**Telnet path:**

**Setup > Interfaces > WLAN > Network**

**Possible values:**

Max. 10 characters from `0123456789`

**Default:**

0

**Special values:**

**0**

Disables the limit.

### Assisted-Roaming

With this setting, you enable Neighbor Reports (802.11k) and Network assisted Roaming (802.11v). When this setting is enabled on both the access point and the client, the client will have more information about its network, thus resulting in better roaming performance.

**SNMP ID:**

2.23.20.1.30

**Telnet path:**

**Setup > Interfaces > WLAN > Network**

**Possible values:**

**No**
**Yes**

**Default:**

Yes

# 5 WLAN-Diagnostics

## Additions to the Setup Menu

### Active

Here you activate the WLAN-Diagnostics table.

**SNMP ID:**

2.12.260.263

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics**

**Possible values:**

Yes
No

**Default:**

No

### Time-Interval (ms)

Here you specify the time interval for recording the entries in the WLAN-Diagnostics table.

**SNMP-ID:**

2.12.260.261.2

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics > Config**

**Possible values:** 200 ms to 60000 ms

**Default:** 1000 ms

### SSID

Here you can specify a SSID that serves as a basis for filtering the entries in the WLAN-Diagnostics table. The Clients connected to that SSID will then be logged in the WLAN-Diagnostics table.
If you do NOT specify any SSID, then the connected Clients in every SSID will be logged.

**SNMP ID:**

2.12.260.262.10

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) Test?0: All clients connected with SSID having any character in place of “?” will be logged (for example Test10, Test20)
2) Test*: All clients connected with SSID starting with “Test” will be logged (for example Test123, Testfirst)

**Default:** No entry

### Lowest-SNR-Clients

Here you specify the number of connected Clients with the lowest SNR that shall be logged in the WLAN-Diagnostics table.
If you set the value to 0, all the connected Clients will be logged in the WLAN-Diagnostics table.

**SNMP ID:**

2.12.260.262.11

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** 0 to 255

**Default:** 3

### Client-Name

Here you can specify the name of a Client that shall be logged in the WLAN-Diagnostics table.
If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

**SNMP ID:**

2.12.260.262.12

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) BAT45?1: All Clients with a name having any character in place of “?” will be logged (for example BAT4501, BAT4521)
2) BAT45*: All Clients with a name starting with “BAT45” will be logged (for example BAT45012, BAT45655)

**Default:** No entry

### Client-MAC

Here you can specify the MAC address of a Client that shall be logged in the WLAN-Diagnostics table.
If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

**SNMP ID:**

2.12.260.262.13

**Telnet path:**

**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) 04:f0:21:33:2c:?d: All Clients with a MAC address having any character in place of “?” will be logged (for example 04:f0:21:33:2c:fd).
2) 04:f0:21:33:2c:*.: All Clients with a MAC address starting with “04:f0:21:33:2c:” will be logged (for example 04:f0:21:33:2c:6d).

**Default:** No entry

**Examples for possible MAC address formats:**
1) 04:f0:21:33:2c:9d
2) 04f021332c9d
3) 04-f0-21-33-2c-9d

### Client-IP

Here you can specify the IP address of a Client that shall be logged in the WLAN-Diagnostics table. If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

**SNMP ID:**
2.12.260.262.14

**Telnet path:**
**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported
Examples for using a wild card:
1) 192.168.10.2?: All Clients with an IP address having any character in place of “?” will be logged (for example 192.168.10.23).
2) 192.168.10.*: All Clients with an IP address starting with “192.168.10.” will be logged (for example 192.168.10.40).

**Default:** No entry

### Highest-SNR-Neighbor-AP

Here you can specify values ranging from 0 to 3. These values represent the number of strongest neighboring Access Points with the event source labeled as 'Neighbor'. When a background scan is initiated, rows containing information about these neighboring Access Points are added to the WLAN Diagnostics table. The value selected determines how many of the strongest neighboring Access Points are included.

**SNMP ID:**
2.12.260.262.15

**Telnet path:**
**Setup > WLAN > WLAN-Diagnostics > Filter**

**Possible values:** 0-3

**Default:** 0

# 6 WLAN-Management

## Additions to the Setup Menu

### PMK-Lifetime-in-sec

Here you can set the PMK lifetime in seconds on the WLC. For instance, setting it to 3600 seconds allows PMKs to last for 1 hour after 802.1x authentication. This means that Clients roaming between Access Points managed by the same WLC won't need full reauthentication until the PMK expires (OKC activation required). PMK configuration is available on the WLC.

**SNMP ID:**

2.37.251

**Telnet path:**

**Setup > WLAN-Management**

**Possible values:**

0 to 4294967295 seconds

**Default:**

1800 seconds (30 minutes)

# 7 Syslog

## Additions to the Setup Menu

### Syslog-with-Milliseconds

Timestamp precision now extends to milliseconds, supplementing the existing second-level precision. Here you can enable or disable this feature.

**SNMP ID:**

2.22.13

**Telnet path:**

**Setup > Syslog**

**Possible values:**

Enable
Disable

**Default:**

Disable

# 8 Interfaces

## 8.1 Channel Indication

With this feature, you can adjust channel priorities for roaming. Indicated channels are moved to the highest priorities according to the chosen channels.

### Additions to the Setup menu

#### Roaming-Indication

Here you enable/disable the Channel Indication feature.

**SNMP ID:**

2.23.20.6.1.14

**Telnet path:**

**Setup > Interfaces > WLAN > Client-Modes > WLAN-1**

**Possible values:**

0 (Disable)
1 (Enable)

**Default:**

0 (Disable)

#### Channel-Indication

Here you can specify up to 5 prioritized channels for roaming.

**SNMP ID:**

2.23.20.6.1.15

**Telnet path:**

**Setup > Interfaces > WLAN > Client-Modes > WLAN-1**

**Possible values:**

Maximum of 5 channels in a comma-separated list.
Example: 36, 100, 108

**Default:**

No entry

## 8.2. Backlobe Patch Antenna Roaming Algorithm

The Backlobe Patch Antenna Roaming Algorithm is designed to address signal degradation issues caused by patch antennas, particularly in scenarios where a Client (e.g., a train) passes an Access Point (AP) and experiences packet loss due to signals being transmitted in the backlobe of the antenna. The solution involves detecting signal drops and triggering a roaming decision to a better AP to maintain connectivity and prevent packet loss.

### Additions to the Setup menu

#### Signal-Drop-Threshold

The Signal-Drop-Threshold is the signal level drop (in dBm) required to trigger a background scan for a new Access Point (AP). When the current connection experiences a signal drop that surpasses this threshold, the roaming algorithm initiates a scan for other APs within range. If a new AP is found, the Client roams to it, and the previous AP is blacklisted for a configurable block time to prevent immediate reconnection.

Here you specify the maximum allowable signal drop before the Client attempts to roam to another AP.

**SNMP ID:**

2.23.20.11.1.12

**Telnet path:**

**Setup > Interfaces > WLAN > Roaming**

**Possible values:**

0 to 255 (dBM)

**Default:**

0 (disabled)

#### Signal-Drop-Active-Threshold

The Signal-Drop-Active-Threshold is a percentage of signal strength that must be met for the Signal-Drop-Threshold detection algorithm to activate. This ensures that the roaming algorithm only triggers when the current signal strength is sufficiently strong, preventing unnecessary background scans at weak signal levels.

Here you can specify the signal strength threshold (in percent) necessary for the current connection to activate the signal drop algorithm.

**SNMP ID:**

2.23.20.11.1.13

**Telnet path:**

**Setup > Interfaces > WLAN > Roaming**

**Possible values:**

0 to 100 (%)

**Default:**

0 (disabled)

HIRSCHMANN

A BELDEN BRAND