Reference Manual

Graphical User Interface
GREYHOUND Switch GRS103
HiOS-2A
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.

© 2022 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

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 find the latest user documentation for your device at: doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
1 Basic Settings
1.1 System . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19
1.2 Modules . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
1.3 Network . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
1.3.1 Global . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
1.3.2 IPv4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29
1.3.3 IPv6 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32
1.4 Out-of-Band over USB . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35
1.5 Software . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38
1.6 Load/Save . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
1.7 External Memory . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53
1.8 Port . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 56
1.9 Power over Ethernet . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 62
1.9.1 PoE Global . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 63
1.9.2 PoE Port . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 65
1.10 Restart . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 68
2 Time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 71
2.1 Basic Settings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 71
2.2 SNTP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 75
2.2.1 SNTP Client . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 76
2.2.2 SNTP Server . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 80
3 Device Security . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 83
3.1 User Management . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 83
3.2 Authentication List . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 89
3.3 LDAP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 92
3.3.1 LDAP Configuration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 93
3.3.2 LDAP Role Mapping . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99
3.4 Management Access . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 101
3.4.1 Server . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 102
3.4.2 IP Access Restriction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115
3.4.3 Web . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 118
3.4.4 Command Line Interface . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
3.4.5 SNMPv1/v2 Community . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
3.5 Pre-login Banner . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 122
5.8.1 VLAN Global ................................................................. 215
5.8.2 VLAN Configuration ................................................. 216
5.8.3 VLAN Port ................................................................. 219
5.8.4 VLAN Voice ............................................................... 220
5.9 L2-Redundancy ............................................................. 223
5.9.1 MRP ........................................................................... 224
5.9.2 Spanning Tree ............................................................. 227
5.9.2.1 Spanning Tree Global .............................................. 228
5.9.2.2 Spanning Tree Port ................................................ 234
5.9.3 Link Aggregation ........................................................ 241
5.9.5 FuseNet ..................................................................... 250
5.9.5.1 Sub Ring ................................................................. 251
6 Diagnostics ................................................................. 257
6.1 Status Configuration ....................................................... 257
6.1.2 Security Status .......................................................... 258
6.1.3 Signal Contact ............................................................ 263
6.1.3.1 Signal Contact 1 / Signal Contact 2 ....................... 269
6.1.4 MAC Notification ....................................................... 275
6.1.5 Alarms (Traps) ............................................................. 277
6.2 System ........................................................................ 279
6.2.1 System Information .................................................... 280
6.2.2 Hardware State .......................................................... 281
6.2.3 Configuration Check ................................................... 282
6.2.4 IP Address Conflict Detection ..................................... 284
6.2.5 ARP ....................................................................... 288
6.2.6 Selftest .................................................................... 290
6.3 Email Notification .......................................................... 292
6.3.1 Email Notification Global ............................................ 293
6.3.2 Email Notification Recipients ...................................... 297
6.3.3 Email Notification Mail Server .................................... 299
6.4 Syslog ........................................................................ 301
6.5 Ports ......................................................................... 305
6.5.1 SFP .................................................................... 306
6.5.2 TP cable diagnosis ...................................................... 307
6.5.3 Port Monitor ............................................................... 309
6.5.4 Auto-Disable ............................................................. 319
6.5.5 Port Mirroring ............................................................. 323
6.6 LLDP ........................................................................ 325
6.6.1 LLDP Configuration .................................................. 326
6.6.2 LLDP Topology Discovery ......................................... 330
6.7 Loop Protection ............................................................. 333
6.8 Report ....................................................................... 338
6.8.1 Report Global ............................................................ 339
6.8.2 Persistent Logging ...................................................... 343
## Contents

| 6.8.3 | System Log | 346 |
| 6.8.4 | Audit Trail | 347 |

### 7 Advanced

| 7.1 | DHCP L2 Relay | 349 |
| 7.1.1 | DHCP L2 Relay Configuration | 349 |
| 7.1.2 | DHCP L2 Relay Statistics | 350 |
| 7.2 | DHCP Server | 354 |
| 7.2.1 | DHCP Server Global | 355 |
| 7.2.2 | DHCP Server Pool | 357 |
| 7.2.3 | DHCP Server Lease Table | 362 |
| 7.3 | DNS | 363 |
| 7.3.1 | DNS Client | 363 |
| 7.3.1.1 | DNS Client Global | 364 |
| 7.3.1.2 | DNS Client Current | 365 |
| 7.3.1.3 | DNS Client Static | 366 |
| 7.3.1.4 | DNS Client Static Hosts | 368 |
| 7.4 | Industrial Protocols | 369 |
| 7.4.1 | IEC61850-MMS | 370 |
| 7.4.2 | Modbus TCP | 373 |
| 7.4.3 | OPC UA Server | 375 |
| 7.5 | Command Line Interface | 378 |

### A Index

- Index | 379 |

### B Further support

- Further support | 383 |

### C Readers' Comments

- Readers' Comments | 384 |
UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.
About this Manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:
- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway
The designations used in this manual have the following meanings:

- **List**
- **Work step**
- **Link** Cross-reference with link
- **Note:** A note emphasizes a significant fact or draws your attention to a dependency.
- **Courier** Representation of a CLI command or field contents in the graphical user interface

- Execution in the Graphical User Interface
- Execution in the Command Line Interface
Notes on the Graphical User Interface

The prerequisite to use the Graphical User Interface of the device is a web browser with HTML5 support.

The responsive Graphical User Interface automatically adapts to the size of your screen. Consequently, you can see more details on a large, high-resolution screen than on a small screen. For example, on a high-resolution screen, the buttons have a label next to the icon. On a screen with a small width, the Graphical User Interface displays only the icon.

**Note:** On a conventional screen, you click to navigate. On a device with a touchscreen, on the other hand, you tap. For simplicity, we only use "click" in our help texts.

The Graphical User Interface is divided as follows:
- Banner
- Menu pane
- Dialog area

Banner

The banner displays the following information:

- Displays and hides the menu. The banner displays the button if the web browser window is too narrow.

Brand logo

Click the logo to open the website of the manufacturer in a new window.

Dialog name

Displays the name of the dialog currently displayed in the dialog area.

Displays that the Graphical User Interface cannot contact the device. The connection to the device is interrupted.

Displays if the settings in the volatile memory (RAM) differ from the settings of the "Selected" configuration profile in the non-volatile memory (NVM). The banner displays the icon if you have transferred the changes to the volatile memory (RAM), but not yet saved them in the non-volatile memory (NVM).
When you click the button, the online help opens in a new window.

When you click the button, a tooltip displays the following information:
- The summary of the Device status frame. See the Basic Settings > System dialog.
- The summary of the Security status frame. See the Basic Settings > System dialog.
- The summary of the Information frame. See the Diagnostics > System > Configuration Check dialog.

A red dot next to the icon means that at least one of the values is greater than 0.

When you click the button, a submenu opens with the following menu items:
- User account name
  The account name of the user that is currently logged in.
- Logout button
  When you click the button, this logs out the currently logged in user. Then the login dialog opens.
Menu pane

The graphical user interface hides the menu pane if the web browser window is too narrow.
To display the menu pane, click the button in the banner.

The menu pane is divided as follows:
- Icons bar
- Menu tree

Icons bar

The icons bar displays the following information:

Device software

Displays the version number of the device software that the device loaded during the last system startup and is currently running.

Displays a text field to search for a keyword. When you enter a character or string, the menu tree displays a menu item only for those dialogs that are related to this keyword.

The menu tree displays a menu item only for those dialogs in which at least one parameter differs from the default setting (Diff to default). To display the complete menu tree again, click the button.

Collapses the menu tree. The menu tree then displays only the menu items of the first level.

Expands the menu tree. The menu tree then displays every menu item on every level.
**Menu tree**

The menu tree contains one item for each dialog in the Graphical User Interface. When you click a menu item, the dialog area displays the corresponding dialog. You can change the view of the menu tree by clicking the buttons in the icons bar at the top. Furthermore, you can change the view of the menu tree by clicking the following buttons:

- **+**
  
  Expands the current menu item to display the menu items of the next lower level. The menu tree displays the button next to each collapsed menu item that contains menu items on the next lower level.

- **-**
  
  Collapses the menu item to hide the menu items of the lower levels. The menu tree displays the button next to each expanded menu item.
Dialog area

The dialog area displays the dialog that you select in the menu tree, including its controls. Here, you can monitor and change the settings of the device depending on your access role.

Below you find useful information on how to use the dialogs.

- Control elements
- Modification mark
- Standard buttons
- Saving the settings
- Updating the display
- Working with tables

Control elements

The dialogs contain different control elements. These control elements are read-only or editable, depending on the parameter and your access role as a user.

The control elements have the following visual properties:

- Input fields
  - An editable input field has a line at the bottom.
  - A read-only input field has no special visual properties.
- Checkboxes
  - An editable checkbox has a bright color.
  - A read-only checkbox has a grey color.
- Radio buttons
  - An editable radio button has a bright color.
  - A read-only radio button has a grey color.

Modification mark

When you modify a value, the corresponding field or table cell displays a red triangle in its top-left corner. The red triangle indicates that you have not yet transferred your modification to the volatile memory (RAM) of the device.

Standard buttons

Here you find the description of the standard buttons. The special dialog-specific buttons are described in the corresponding dialog help text.

✓ Transfers the changes to the volatile memory (RAM) of the device and applies them to the device.

Information on how the device retains the modified settings even after a reboot you find in section “Saving the settings” on page 16.
Undoes the unsaved changes in the current dialog. Updates the fields with the values that are saved in the volatile memory (RAM) of the device.

**Saving the settings**

Saving transfers the modified settings to the volatile memory (RAM) of the device. To do this, perform the following step:

- Click the ✓ button.

**Note:** Unintentional changes to the settings can terminate the connection between your PC and the device. To keep the device accessible, enable the *Undo configuration modifications* function in the **Basic Settings > Load/Save** dialog, before changing any settings. Using the function, the device continuously checks if it can still be reached from the IP address of your PC. If the connection is lost, then the device loads the configuration profile saved in the non-volatile memory (NVM) after the specified time. Afterwards, the device can be accessed again.

To keep the modified settings even after restarting the device, perform the following steps:

- Open the **Basic Settings > Load/Save** dialog.
- In the table, mark the checkbox far left in the table row of the desired configuration profile.
- When the checkbox in the *Selected* column is unmarked, click the ☑ button and then the *Select* item.
- Click the ✓ button to save your current changes.

**Updating the display**

If a dialog remains open for a longer time, then the values in the device have possibly changed in the meantime.

- To update the display in the dialog, click the ✓ button. Unsaved information in the dialog is lost.

**Working with tables**

The dialogs display numerous settings in table form. You have the option of customizing the appearance of the tables to fit your needs.

You can find useful information on how to use the tables in the following sections:

- Filter rows
- Sort rows
- Select multiple table rows
**Filter rows**

The filter lets you reduce the number of displayed table rows.

Displays a second table row in the table header containing a text field for every column. When you enter a string in a field, the table displays only the table rows that contain this string in the corresponding column.

**Sort rows**

Every column in the table header contains an icon that lets you change the order of the table rows.

Displays that the table rows are sorted by a criterion other than the values in this column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging off and logging in again.

Displays that the table rows are sorted in ascending order based on the entries of the corresponding column.

Click the icon to sort the table rows in ascending order based on the entries of the corresponding column.

Displays that the table rows are sorted in descending order based on the entries of the corresponding column.

Click the icon to sort the table rows in descending order based on the entries of the corresponding column.

**Select multiple table rows**

You have the option of selecting multiple table rows at once and then apply an action to them. This is useful for example, when you want to remove multiple table rows at the same time.

To select individual table rows, mark the leftmost checkbox in the desired table row.

To select every table row, mark the leftmost checkbox in the table header.
1 Basic Settings

The menu contains the following dialogs:
- System
- Modules
- Network
- Out-of-Band over USB
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet
- Restart

1.1 System

This dialog displays information about the operating status of the device.

Device status

Displays the device status and the alarms that currently exist. When at least 1 alarm is present, the background color is red. Otherwise, the background color is green.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Device Status dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the Diagnostics > Status Configuration > Device Status dialog, the Status tab displays an overview of the alarms.

Note: If you connect only 1 power supply unit to a device that supports 2 redundant power supply units, then the device reports an alarm. To disable this kind of alarm, deactivate the monitoring of the missing power supply units in the Diagnostics > Status Configuration > Device Status dialog.
**Security status**

Displays the security status and the alarms that currently exist. When at least 1 alarm is present, the background color is red. Otherwise, the background color is green.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Security Status dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the Diagnostics > Status Configuration > Security Status dialog, the Status tab displays an overview of the alarms.

**Signal contact status**

The device can contain several signal contacts.

Displays the signal contact status and the alarms that currently exist. When at least 1 alarm is present, the background color is red. Otherwise, the background color is green.

You specify the parameters that the device monitors in the Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Diagnostics > Status Configuration > Signal Contact > Signal Contact 2 dialog. If a monitored parameter differs from the desired status, then the device triggers an alarm.

A tooltip displays the cause of the currently existing alarms and the time at which the device triggered the alarm. To display the tooltip, hover the mouse pointer over or tap the field. In the Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Diagnostics > Status Configuration > Signal Contact > Signal Contact 2 dialog, the Status tab displays an overview of the alarms.

**System data**

The fields in this frame display operating data and information on the location of the device.

**System name**

Specifies the name by which the device is known in the network.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  The device accepts the following characters:
  - 0..9
  - a..z
  - A..Z
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~
  <device type name>-<MAC address>  (default setting)
When creating HTTPS X.509 certificates, the application generating the certificate uses the specified value as the domain name and common name.

The following functions use the specified value as a host name or FQDN (Fully Qualified Domain Name). For compatibility, it is recommended to use only lowercase letters, since some systems distinguish uppercase from lowercase in the FQDN. Verify that this name is unique in the whole network.

- DHCP client
- Syslog
- IEC61850-MMS

**Location**

Specifies the current or planned location.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

**Contact person**

Specifies the contact person for this device.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

**Device type**

Displays the product name of the basic device.

**Power supply 1**  
**Power supply 2**

Displays the status of the power supply unit at the respective voltage supply connector.

Possible values:
- present
- defective
- not installed
- unknown

**Uptime**

Displays the time that has elapsed since the device was last restarted.

Possible values:
- Time in the format `day(s), ...h ...m ...s`

**Temperature [°C]**

Displays the current temperature in the device in °C.

You activate the monitoring of the temperature threshold values in the Diagnostics > Status Configuration > Device Status dialog.
Upper temp. limit [°C]

Specifies the upper temperature threshold value in °C.

Possible values:

► -99...99 (integer)

If the temperature in the device exceeds the specified value, then the device displays an alarm.

Lower temp. limit [°C]

Specifies the lower temperature threshold value in °C.

Possible values:

► -99...99 (integer)

If the temperature in the device falls below the specified value, then the device displays an alarm.

**LED status**

For further information about the device status LEDs, see the "Installation" user manual.

**Status**

- There is currently no device status alarm. The device status is OK.

- There is currently at least 1 device status alarm. For details, see the Device status frame.

**Power**

- Device that supports 2 redundant power supply units: Only 1 supply voltage is active.

- Device that supports 1 power supply unit: The supply voltage is active.

- Device that supports 2 redundant power supply units: Both supply voltages are active.

**ACA**

- No external memory connected.
The external memory is connected, but not ready for operation.

The external memory is connected and ready for operation.

**Port status**

This frame displays a simplified view of the device ports at the time of the last display update. In the initial view, the frame only displays ports with an active link. When you click the button, the frame displays every port.

You can easily identify the port status from the indicator:

- **Ports with an active link:**
  - The background color is green.
  - The port speed is displayed next to the port number.
- **Ports with an inactive link:**
  - The background color is gray.
- **Ports in a **Blocking** state due to a redundancy function:**
  - The border is dashed.

When you hover the mouse pointer over or tap the appropriate port icon, a tooltip displays detailed port state information.
1.2 Modules

The device lets you install or remove the modules during operation (hot-plug).

As long as the Ethernet module status column displays the value configurable you can configure the module and save its preferences.

- When you replace the module with an identical module, the device applies the settings to the new module immediately.
- When you replace the module with a different type of module, the device applies the factory settings to the new module.
- When you plug a module in an empty slot, the device configures the module with its default settings. If the slot is inactive, then it remains inactive until you mark the checkbox in the Active column. With the port default settings loaded on the module, access to the network is possible.

Install an Ethernet module

Perform the following steps:

- Plug the module in the slot.
  The device automatically configures the module with the default settings, and detects the module parameters.
- To update the Graphical User Interface, click the кнопка. The Ethernet module status column displays the value physical for the installed Ethernet module.
- Save the settings temporarily. To do this, click the кнопка.

Activate/Deactivate a slot

On an inactive slot, the device recognizes the installed module and port configuration is possible. The module establishes no network connections on a inactive slot.

Perform the following steps:

- Select the table row of the module.
- To deactivate the slot and deny network access, unmark the Active checkbox.
- To activate the slot and allow network access, mark the Active checkbox.
- Save the settings temporarily. To do this, click the кнопка.

Remove an Ethernet module

Perform the following steps:

- Remove the module from the slot.
- To update the Graphical User Interface, click the кнопка. The Ethernet module status column displays the value configurable for the removed module.
- Select the table row of the removed module.
- Click the кнопка. The Ethernet module status column displays the value remove for the removed module. The Type column and some other columns display the value n/a. The marked Active checkbox indicates that the slot is still active.
- Save the settings temporarily. To do this, click the кнопка.
**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Remove Ethernet module**
  
  Removes the selected Ethernet module from the table.

**Ethernet module**

Displays the number of the slot to which the table row refers.

**Active**

Activates/deactivates the slot.

Possible values:

- **marked**  (default setting)  
  The slot is active. The device recognizes a module installed in this slot.

- **unmarked**  
  The slot is inactive.

**Type**

Displays the type of the installed module.

A value of *n/a* indicates that the slot is empty.

**Description**

Specifies a short description of the installed module.

**Version**

Displays the version of the installed module.

**Ports**

Displays how many ports are available on the installed module.

**Serial number**

Displays the serial number of the installed module.

A value of *n/a* indicates that the slot is empty.
Ethernet module status

Displays the status of the slot.

Possible values:

- **physical**
  A module is present in the slot.

- **configurable**
  The slot is empty and available for configuration.

- **remove**
  The slot is empty and inactive.

- **fix**
  The module cannot be removed.

### 1.3 Network

The menu contains the following dialogs:

- **Global**
- **IPv4**
- **IPv6**
1.3.1 Global

This dialog lets you specify the VLAN and HiDiscovery settings required for the access to the device management through the network.

Management interface

This frame lets you specify the VLAN in which the device management can be accessed.

VLAN ID

Specifies the VLAN in which the device management is accessible through the network. The device management is accessible through ports that are members of this VLAN.

Possible values:

- 1..4042 (default setting: 1)
  - The prerequisite is that in the Switching > VLAN > Configuration dialog the VLAN is already set up.

When you click the ✓ button after changing the value, the Information window opens. Select the port, over which you connect to the device in the future. After clicking the Ok button, the new device management VLAN settings are assigned to the port.

- After that the port is a member of the VLAN and transmits the data packets without a VLAN tag (untagged). See the Switching > VLAN > Configuration dialog.
- The device assigns the port VLAN ID of the device management VLAN to the port. See the Switching > VLAN > Port dialog.

After a short time the device is reachable over the new port in the new device management VLAN.

MAC address

Displays the MAC address of the device. The device management is accessible through the network using the MAC address.

HiDiscovery protocol v1/v2

This frame lets you specify settings for the access to the device using the HiDiscovery protocol.

On a PC, the HiDiscovery software displays the Hirschmann devices that can be accessed in the network on which the HiDiscovery function is enabled. You can access these devices even if they have invalid or no IP parameters assigned. The HiDiscovery software lets you assign or change the IP parameters in the device.

Note: With the HiDiscovery software you access the device only through ports that are members of the same VLAN as the device management. You specify which VLAN a certain port is assigned to in the Switching > VLAN > Configuration dialog.
Basic Settings

[Basic Settings > Network > Global]

Operation

Enables/disables the HiDiscovery function in the device.

Possible values:

- **On** (default setting)
  - The HiDiscovery function is enabled.
  - You can use the HiDiscovery software to access the device from your PC.

- **Off**
  - The HiDiscovery function is disabled.

Access

Enables/disables the write access to the device using for the HiDiscovery function.

Possible values:

- **readWrite** (default setting)
  - The HiDiscovery function has write access to the device. The device lets you change the IP parameters in the device using the HiDiscovery function.

- **readOnly**
  - The HiDiscovery function has read-only access to the device. The device lets you view the IP parameters in the device using the HiDiscovery function.

Recommendation: Change the setting to the value **readOnly** only after putting the device into operation.

Signal

Activates/deactivates the flashing of the port LEDs as does the function of the same name in the HiDiscovery software. The function lets you identify the device in the field.

Possible values:

- **marked**
  - The flashing of the port LEDs is active.
  - The port LEDs flash until you disable the function again.

- **unmarked** (default setting)
  - The flashing of the port LEDs is inactive.
1.3.2 IPv4

This dialog allows you to specify the IPv4 settings required for the access to the device management through the network.

Management interface

IP address assignment

Specifies the source from which the device management receives its IP parameters.

Possible values:

- **Local**
  The device uses the IP parameters from the internal memory. You specify the settings for this in the IP parameter frame.

- **BOOTP**
  The device receives its IP parameters from a BOOTP or DHCP server.
  The server evaluates the MAC address of the device, then assigns the IP parameters.

- **DHCP** (default setting)
  The device receives its IP parameters from a DHCP server.
  The server evaluates the MAC address, the DHCP name, or other parameters of the device, then assigns the IP parameters.
  When the server also provides the addresses of DNS servers, the device displays these addresses in the Advanced > DNS > Client > Current dialog.

**Note:** If there is no response from the BOOTP or DHCP server, then the device sets the IP address to 0.0.0.0 and makes another attempt to obtain a valid IP address.
**IP parameter**

This frame lets you assign the IP parameters manually. If you have selected the *Local* radio button in the *Management interface* frame, *IP address assignment* option list, then these fields can be edited.

**IP address**

Specifies the IP address under which the device management can be accessed through the network.

Possible values:
- Valid IPv4 address

**Netmask**

Specifies the netmask.

Possible values:
- Valid IPv4 netmask

**Gateway address**

Specifies the IP address of a router through which the device accesses other devices outside of its own network.

Possible values:
- Valid IPv4 address

**BOOTP/DHCP**

**Client ID**

Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is configured accordingly, then it reserves an IP address for this DHCP client ID. Therefore, the device receives the same IP from the server every time it requests it.

The DHCP client ID that the device sends is the device name specified in the *System name* field in the *Basic Settings > System* dialog.
DHCP option 66/67/4/42

Enables/disables the **DHCP option 66/67/4/42** function in the device.

Possible values:

- **On** (default setting)
  The **DHCP option 66/67/4/42** function is enabled.
  The device loads the configuration profile and receives the time server information using the following DHCP options:
  - Option 66: TFTP server name
  - Option 67: Boot file name
    The device automatically loads the configuration profile from the DHCP server into the volatile memory (RAM) using the TFTP protocol. The device uses the settings of the imported configuration profile in the **running-config**.
  - Option 4: Time Server
  - Option 42: Network Time Protocol Servers
    The device receives the time server information from the DHCP server.

- **Off**
  The **DHCP option 66/67/4/42** function is disabled.
  - The device does not load a configuration profile using DHCP Options 66/67.
  - The device does not receive time server information using DHCP Options 4/42.

Remaining lease time

**Lease time [s]**

Displays the remaining time in seconds during which the IP address that the DHCP server assigned to the device management is still valid.

To update the display, click the **button.**
1.3.3 IPv6

This dialog allows you to specify the IPv6 settings required for the access to the device management through the network.

**Operation**

Enables/disables the IPv6 protocol in the device.

Both IPv4 and IPv6 protocols can operate at the same time in the device. This is possible with the use of the Dual IP Layer technique, also referred to as Dual Stack.

Possible values:

- **On** (default setting)
  - The IPv6 protocol is enabled.
- **Off**
  - The IPv6 protocol is disabled.
  - If you want the device to operate only using the IPv4 protocol, then disable the IPv6 protocol in the device.

**Configuration**

Dynamic IP address assignment

Specifies the source from which the device management receives its IPv6 parameters.

Possible values:

- **None**
  - The device receives its IPv6 parameters manually.
  - You can manually specify a maximum number of 4 IPv6 addresses. You cannot specify loopback, link-local, and Multicast addresses as static IPv6 addresses.
- **Auto** (default setting)
  - The device receives its IPv6 parameters dynamically. The device receives a maximum of 2 IPv6 addresses.
  - An example here is the Router Advertisement Daemon (radvd). The radvd uses Router Solicitation and Router Advertisement messages to automatically configure an IPv6 address. The Router Solicitation and Router Advertisement messages are described in RFC 4861.
- **DHCPv6**
  - The device receives its IPv6 parameters from a DHCPv6 server.
- **All**
  - If the All radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.


**DHCP**

**Client ID**

Displays the DHCPv6 client ID that the device sends to the DHCPv6 server. If the server is configured accordingly, then it receives an IPv6 address for this DHCPv6 client ID.

The IPv6 address received from the DHCPv6 server has a *PrefixLength* of 128. According to RFC 8415, at the moment a DHCPv6 server cannot be used to supply *Gateway address* or *PrefixLength* information.

The device can receive only one IPv6 address from the DHCPv6 server.

**IP parameter**

**Gateway address**

Specifies the IPv6 address of a router through which the device accesses other devices outside its own network.

Possible values:

- Valid IPv6 address (except loopback and Multicast addresses)

*Note:* If the *Auto* radio button is selected and you use a Router Advertisement Daemon (radvd), then the device automatically receives a link-local type *Gateway address* with a higher metric than the manually set *Gateway address*.

**Duplicate Address Detection**

In this field you can specify the number of consecutive Neighbor Solicitation messages that the device sends for the *Duplicate Address Detection* function. This function is used to determine the uniqueness of an IPv6 unicast address on the interface.

**Number of neighbor solicitants**

Specifies the number of Neighbor Solicitation messages that the device sends for the *Duplicate Address Detection* function.

Possible values:

- 0   The function is disabled.
- 1..5 (default setting: 1)

If the *Duplicate Address Detection* function discovers that an IPv6 address is not unique on a link, then the device does not log this event in the log file (System Log).
Table

This table displays a list of the IPv6 addresses configured for the device management.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Prefix

Displays the prefix of the IPv6 address in a compressed format. The prefix shows the leftmost bits of an IPv6 address, also known as the network part of the address.

PrefixLength

Displays the prefix length of the IPv6 address.

Unlike an IPv4 address, the IPv6 address does not use a subnet mask to identify the network part of an address. This role is performed in IPv6 by the prefix length.

Possible values:

- 0..128

IP address

Displays the full IPv6 address in a compressed format.

The compressed format is automatically applied to every IPv6 address, regardless of the source from which the device management receives its IPv6 parameters.

Possible values:

- Valid IPv6 address
  - To use an IPv6 address in a URL, use the following URL syntax: https://[<ipv6_address>].

For further information on IPv6 compression rules and address types, see the “Configuration” user manual.

EUI option

Specifies if the **EUI option** function is applied to the IPv6 address.

When you mark this checkbox, the Interface ID of the IPv6 address is automatically configured. The device uses the MAC address of its interface with the values ff and fe added between byte 3 and byte 4 to generate a 64-bit Interface ID.

You can only select this option for IPv6 addresses that have a prefix length equal to 64.

Possible values:

- **marked**
  - The **EUI option** function is active.
- **unmarked** (default setting)
  - The **EUI option** function is inactive.
## Origin

Specifies the way in which the device received its IPv6 parameters.

Possible values:

- **Autoconf**
  The device received the IPv6 address dynamically, when the *Auto* radio button is selected.
- **Manual**
  The device received the IPv6 address manually.
- **DHCP**
  The device received the IPv6 address from a DHCPv6 server.
- **Linklayer**
  The device automatically configures a link-local type IPv6 address. The link-local address cannot be changed.

## Status

Displays the current status of the IPv6 address.

Possible values:

- **active**
  The IPv6 address is active.
- **notInService**
  The IPv6 address is inactive.
- **notReady**
  The IPv6 address is specified, but not currently active as some configuration parameters are still missing.

**Note:** When the IPv6 address is manually specified, you can manually change between *active* and *notInService* states. To do this, for the corresponding table row, select in the *Status* column the desired status from the drop-down list.

### 1.4 Out-of-Band over USB

The device comes with a USB network interface that lets you access the device management out-of-band. When there is a high in-band load on the switching ports, you can still use the USB network interface to access the device management.

The device lets you access the device management through the USB network interface using the following protocols:

- HTTP
- HTTPS
- SSH
- Telnet
- SNMP
- FTP
- TFTP
- SFTP
- SCP
When accessing the device management there are the following limitations:

- The management station is directly connected to the USB port.
- The USB network interface does not support the following features:
  - Priority tagged packets
  - Packets including a VLAN tag
  - DHCP L2 Relay
  - LLDP
  - DiffServ
  - ACL
  - Industrial Protocols

In this dialog the device lets you change the IP parameters and disable the USB network interface, if needed.

**Operation**

Enables/disables the USB network interface.

Possible values:

- **On** (default setting)
  - The device lets you access the device management through the USB network interface.
- **Off**
  - The device prohibits access to the device management through the USB network interface.

**Management interface**

Device MAC address

Displays the MAC address of the USB network interface.

Host MAC address

Displays the MAC address of the connected management station.
**IP parameter**

Verify that the IP subnet of this network interface is not overlapping with any subnet connected to another interface of the device:

- management interface

**IP address**

Specifies the IP address of the device management for access through the USB network interface.

Possible values:

- Valid IPv4 address
  (default setting: 192.168.248.100)
  The device assigns this IP address, increased by 1, to the management station which is connected to the device.

**Netmask**

Specifies the netmask.

Possible values:

- Valid IPv4 netmask
  (default setting: 255.255.255.0)
1.5 **Software**

This dialog lets you update the device software and display information about the device software. You also have the option to restore a backup of the device software saved in the device.

**Note:** Before updating the device software, follow the version-specific notes in the *Readme* text file.

**Version**

**Stored version**

Displays the version number and creation date of the device software stored in the flash memory. The device loads the device software during the next system startup.

**Running version**

Displays the version number and creation date of the device software that the device loaded during the last system startup and is currently running.

**Backup version**

Displays the version number and creation date of the device software saved as a backup in the flash memory. The device copied this device software into the backup memory during the last software update or after you clicked the *Restore* button.

**Restore**

Restores the device software saved as a backup. In the process, the device changes the *Stored version* and the *Backup version* of the device software.

During the next system startup, the device loads the device software displayed in the *Stored version* field.

**Bootcode**

Displays the version number and creation date of the boot code.
Software update

Alternatively, when the image file is located in the external memory, the device lets you update the device software by right-clicking in the table.

URL

Specifies the path and the file name of the image file with which you update the device software.

The device gives you the following options for updating the device software:

- **Software update from the PC**
  
  When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file.

- **Software update from an FTP server**
  
  When the file is located on an FTP server, specify the URL for the file in the following form:
  
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`

- **Software update from a TFTP server**
  
  When the file is located on a TFTP server, specify the URL for the file in the following form:
  
  `tftp://<IP address>/<path>/<file name>`

- **Software update from an SCP or SFTP server**
  
  When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  
  - `scp://<IP address>/<path>/<file name>`
  
  When you click the **Start** button, the device displays the **Credentials** window. There you enter **User name** and **Password**, to log in to the server.
  
  - `scp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Updates the device software.

The device installs the selected file in the flash memory, replacing the previously saved device software. During the next system startup, the device loads the installed device software.

The device copies the existing software into the backup memory.

To remain logged in to the device during the software update, move the mouse pointer occasionally. Alternatively, specify a sufficiently high value in the **Device Security > Management Access > Web** dialog, field **Web interface session timeout [min]** before the software update.

Table

**File location**

Displays the storage location of the device software.

Possible values:

- **ram**
  
  Volatile memory of the device

- **flash**
  
  Non-volatile memory (NVM) of the device

- **usb**
  
  External USB memory (ACA21/ACA22)
Index

Displays the index of the device software.

For the device software in the flash memory, the index has the following meaning:

1. During the next system startup, the device loads this device software.
2. The device copied this device software into the backup area during the last software update.

File name

Displays the device-internal file name of the device software.

Firmware

Displays the version number and creation date of the device software.
1.6 Load/Save

This dialog lets you save the device settings permanently in a configuration profile.

The device can hold several configuration profiles. When you activate an alternative configuration profile, you change to other device settings. You have the option of exporting the configuration profiles to your PC or to a server. You also have the option of importing the configuration profiles from your PC or from a server to the device.

In the default setting, the device saves the configuration profiles unencrypted. If you enter a password in the Configuration encryption frame, then the device saves both the current and the future configuration profiles in an encrypted format.

Unintentional changes to the settings can terminate the connection between your PC and the device. To keep the device accessible, enable the Undo configuration modifications function before changing any settings. If the connection is lost, then the device loads the configuration profile saved in the non-volatile memory (NVM) after the specified time.

Note: Upgrading from Classic to HiOS? Convert your device configuration files using our online tool: https://convert.hirschmann.com

External memory

Selected external memory

Displays the type of the external memory.

Possible values:

- **usb**
  - External USB memory (ACA21/ACA22)

Status

Displays the operating state of the external memory.

Possible values:

- **notPresent**
  - No external memory connected.
- **removed**
  - Someone has removed the external memory from the device during operation.
- **ok**
  - The external memory is connected and ready for operation.
- **outOfMemory**
  - The memory space is occupied in the external memory.
- **genericErr**
  - The device has detected an error.
**Basic Settings > Load/Save**

---

**Configuration encryption**

**Active**

Displays if the configuration encryption is active/inactive in the device.

**Possible values:**

- **marked**
  - The configuration encryption is active.
  - If the configuration profile is encrypted and the password matches the password stored in the device, then the device loads a configuration profile from the non-volatile memory (NVM).

- **unmarked**
  - The configuration encryption is inactive.
  - If the configuration profile is unencrypted, then the device loads a configuration profile from the non-volatile memory (NVM) only.

If in the **Basic Settings > External Memory** dialog, the **Config priority** column has the value **first** and the configuration profile is unencrypted, then the **Security status** frame in the **Basic Settings > System** dialog displays an alarm.

In the **Diagnostics > Status Configuration > Security Status** dialog, **Global** tab, **Monitor** column you specify if the device monitors the **Load unencrypted config from external memory** parameter.

**Set password**

Opens the **Set password** window that helps you to enter the password needed for the configuration profile encryption. Encrypting the configuration profiles makes unauthorized access more difficult.

To do this, perform the following steps:

1. When you are changing an existing password, enter the existing password in the **Old password** field. To display the password in plain text instead of **** (asterisks), mark the **Display content** checkbox.
2. In the **New password** field, enter the password. To display the password in plain text instead of **** (asterisks), mark the **Display content** checkbox.
3. Mark the **Save configuration afterwards** checkbox to use encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory.

**Note:** If a maximum of one configuration profile is stored in the non-volatile memory (NVM) of the device, then use this function only. Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.

If you are replacing a device with an encrypted configuration profile, for example due to an inoperative device, then perform the following steps:

1. Restart the new device and assign the IP parameters.
2. Open the **Basic Settings > Load/Save** dialog on the new device.
3. Encrypt the configuration profile in the new device. See above. Enter the same password you used in the inoperative device.
4. Install the external memory from the inoperative device in the new device.
5. Restart the new device.
   - During the next system startup, the device loads the configuration profile with the settings of the inoperative device from the external memory. The device copies the settings into the volatile memory (RAM) and into the non-volatile memory (NVM).
Delete

Opens the Delete window which helps you to cancel the configuration encryption in the device. To cancel the configuration encryption, perform the following steps:

- In the Old password field, enter the existing password. To display the password in plain text instead of ***** (asterisks), mark the Display content checkbox.
- Mark the Save configuration afterwards checkbox to remove the encryption also for the Selected configuration profile in the non-volatile memory (NVM) and in the external memory.

Note: If you keep additional encrypted configuration profiles in the memory, then the device helps prevent you from activating or designating these configuration profiles as “Selected”.

Undo configuration modifications

Operation

Enables/disables the Undo configuration modifications function. Using the function, the device continuously checks if it can still be reached from the IP address of your PC. If the connection is lost, after a specified time period the device loads the “Selected” configuration profile from the non-volatile memory (NVM). Afterwards, the device can be accessed again.

Possible values:

- **On**
  - The function is enabled.
  - You specify the time period between the interruption of the connection and the loading of the configuration profile in the Timeout [s] to recover after connection loss field.
  - When the non-volatile memory (NVM) contains multiple configuration profiles, the device loads the configuration profile designated as “Selected”.

- **Off** (default setting)
  - The function is disabled.
  - Disable the function again before you close the Graphical User Interface. You thus help prevent the device from restoring the configuration profile designated as “Selected”.

Note: Before you enable the function, save the settings in the configuration profile. The device thus maintains the current settings, that are only temporarily saved.

Timeout [s] to recover after connection loss

Specifies the time in seconds after which the device loads the “Selected” configuration profile from the non-volatile memory (NVM) if the connection is lost.

Possible values:

- **30..600** (default setting: 600)

Specify a sufficiently large value. Take into account the time when you are viewing the dialogs of the Graphical User Interface without changing or updating them.
Watchdog IP address

Displays the IP address of the PC on which you have enabled the function.

Possible values:
- IPv4 address  (default setting: 0.0.0.0)

Information

NVM in sync with running config

Displays if the settings in the volatile memory (RAM) differ from the settings of the "Selected" configuration profile in the non-volatile memory (NVM).

Possible values:
- marked
  The settings match.
- unmarked
  The settings differ. Additionally, the Banner displays the icon 🗣.

External memory in sync with NVM

Displays if the settings of the "Selected" configuration profile in the external memory (ACA) differ from the settings of the "Selected" configuration profile in the non-volatile memory (NVM).

Possible values:
- marked
  The settings match.
- unmarked
  The settings differ.
Possible causes:
- No external memory is connected to the device.
- In the Basic Settings > External Memory dialog, the Backup config when saving function is disabled.

Backup config on a remote server when saving

Operation

Enables/disables the Backup config on a remote server when saving function.

Possible values:
- Enabled
  The Backup config on a remote server when saving function is enabled.
  When you save the configuration profile in the non-volatile memory (NVM), the device automatically backs up the configuration profile on the remote server specified in the URL field.
- Disabled  (default setting)
  The Backup config on a remote server when saving function is disabled.
URL

Specifies path and file name of the backed up configuration profile on the remote server.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters
  Example: tftp://192.9.200.1/cfg/config.xml

The device supports the following wildcards:
- %d
  System date in the format YYYY-mm-dd
- %t
  System time in the format HH_MM_SS
- %i
  IP address of the device
- %m
  MAC address of the device in the format AA-BB-CC-DD-EE-FF
- %p
  Product name of the device

Set credentials

Opens the Credentials window which helps you to enter the login credentials needed to authenticate on the remote server. To do this, perform the following steps:

- In the User name field, enter the user name.
  To display the user name in plain text instead of ***** (asterisks), mark the Display content checkbox.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters

- In the Password field, enter the password.
  To display the password in plain text instead of ***** (asterisks), mark the Display content checkbox.
  Possible values:
  - Alphanumeric ASCII character string with 6..64 characters

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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Remove

Removes the configuration profile selected in the table from the non-volatile memory (NVM) or from the external memory.

If the configuration profile is designated as "Selected", then the device helps prevent you from removing the configuration profile.
Save

Transfers the settings from the volatile memory (RAM) into the configuration profile designated as “Selected” in the non-volatile memory (NVM).

When in the Basic Settings > External Memory dialog the checkbox in the Backup config when saving column is marked, then the device generates a copy of the configuration profile in the external memory.

Save as..

Displays a context menu with further functions for the corresponding dialog.

Opens the Save as.. window to copy the configuration profile selected in the table and saves it with a user-specified name in the non-volatile memory (NVM).

- In the Profile name field, enter the name under which you want to save the configuration profile.
  - To save the configuration profile under a new name, click the button.
  - To overwrite an existing configuration profile, select the corresponding item from the drop-down list.

If in the Basic Settings > External Memory dialog the checkbox in the Backup config when saving column is marked, then the device designates the configuration profile of the same name in the external memory as “Selected”.

Note: Before creating additional configuration profiles, decide for or against permanently activated configuration encryption in the device. Save additional configuration profiles either unencrypted or encrypted with the same password.

Activate

Loads the settings of the configuration profile selected in the table to the volatile memory (RAM).

- The device terminates the connection to the Graphical User Interface. To access the device management again, perform the following steps:
  - Reload the Graphical User Interface.
  - Log in again.
- The device immediately uses the settings of the configuration profile on the fly.

Enable the Undo configuration modifications function before you activate another configuration profile. If the connection is lost afterwards, then the device loads the last configuration profile designated as “Selected” from the non-volatile memory (NVM). The device can then be accessed again.

If the configuration encryption is inactive, then the device loads an unencrypted configuration profile. If the configuration encryption is active and the password matches the password stored in the device, then the device loads an encrypted configuration profile.

When you activate an older configuration profile, the device takes over the settings of the functions contained in this software version. The device sets the values of new functions to their default value.
Select

Designates the configuration profile selected in the table as “Selected”. In the Selected column, the checkbox is then marked.

When applying the Undo configuration modifications function or during the system startup, the device loads the settings of this configuration profile to the volatile memory (RAM).

- If the configuration encryption in the device is disabled, then designate an unencrypted configuration profile only as “Selected”.
- If the configuration encryption in the device is enabled and the password of the configuration profile matches the password saved in the device, then designate an encrypted configuration profile only as “Selected”.

Otherwise, the device is unable to load and encrypt the settings in the configuration profile the next time it restarts. For this case you specify in the Diagnostics > System > Selftest dialog if the device starts with the default settings or terminates the restart and stops.

**Note:** You only mark the configuration profiles saved in the non-volatile memory (NVM).

If in the Basic Settings > External Memory dialog the checkbox in the Backup config when saving column is marked, then the device designates the configuration profile of the same name in the external memory as “Selected”.

Import...

Opens the Import... window to import a configuration profile.

The prerequisite is that you have exported the configuration profile using the Export... button or using the link in the Profile name column.

- From the Select source drop-down list, select from where the device imports the configuration profile.
  - PC/URL
    - The device imports the configuration profile from the local PC or from a remote server.
  - External memory
    - The device imports the configuration profile from the external memory.

- When PC/URL is selected above, in the Import profile from PC/URL frame you specify the configuration profile file to be imported.
  - Import from the PC
    - When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file.
  - Import from an FTP server
    - When the file is located on an FTP server, specify the URL for the file in the following form: ftp://<user>:<password>@<IP address>:<port>/<file name>
  - Import from a TFTP server
    - When the file is located on a TFTP server, specify the URL for the file in the following form: tftp://<IP address>/<path>/<file name>
  - Import from an SCP or SFTP server
    - When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
      - scp://<IP address>/<path>/<file name>
      - sftp://<user>:<password>@<IP address>/<path>/<file name>
    - When you click the Start button, the device displays the Credentials window. There you enter User name and Password, to log in to the server.
      - scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>
When External memory is selected above, in the Import profile from external memory frame you specify the configuration profile file to be imported. From the Profile name drop-down list, select the name of the configuration profile to be imported.

In the Destination frame you specify where the device saves the imported configuration profile. In the Profile name field you specify the name under which the device saves the configuration profile. In the Storage type field you specify the storage location for the configuration profile. The prerequisite is that from the Select source drop-down list the PC/URL item is selected.

RAM
The device saves the configuration profile in the volatile memory (RAM) of the device. This replaces the running-config, the device uses the settings of the imported configuration profile immediately. The device terminates the connection to the Graphical User Interface. Reload the Graphical User Interface. Log in again.

NVM
The device saves the configuration profile in the non-volatile memory (NVM) of the device.

When you import a configuration profile, the device takes over the settings as follows:

- If the configuration profile was exported on the same device or on an identically equipped device of the same type, then:
  The device takes over the settings completely.
  If the device uses modules, then also read the help text of the Basic Settings > Modules dialog.

- If the configuration profile was exported on an other device, then:
  The device takes over the settings which it can interpret based on its hardware equipment and software level.
  The remaining settings the device takes over from its running-config configuration profile.

Regarding configuration profile encryption, also read the help text of the Configuration encryption frame. The device imports a configuration profile under the following conditions:

- The configuration encryption of the device is inactive. The configuration profile is unencrypted.
- The configuration encryption of the device is active. The configuration profile is encrypted with the same password that the device currently uses.

Export...
Exports the configuration profile selected in the table and saves it as an XML file on a remote server.

To save the file on your PC, click the link in the Profile name column to select the storage location and specify the file name.

The device gives you the following options for exporting a configuration profile:

- Export to an FTP server
  To save the file on an FTP server, specify the URL for the file in the following form:
  ftp://<user>:<password>@<IP address>:<port>/<file name>

- Export to a TFTP server
  To save the file on a TFTP server, specify the URL for the file in the following form:
  tftp://<IP address>/<path>/<file name>

- Export to an SCP or SFTP server
  To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    - scp:// or sftp://<IP address>/<path>/<file name>
      When you click the Ok button, the device displays the Credentials window. There you enter User name and Password, to log in to the server.
    - scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>
Save running-config as script

Saves the *running-config* configuration profile as a script file on the local PC. This lets you backup your current device settings or to use them on various devices.

Load running-config as script

Imports a script file which modifies the current *running-config* configuration profile.

The device gives you the following options to import a script file:

- Import from the PC
  When the file is located on your PC or on a network drive, drag and drop the file in the area. Alternatively click in the area to select the file.
- Import from an FTP server
  When the file is located on an FTP server, specify the URL for the file in the following form:
  \`ftp://<user>:<password>@<IP address>:<port>/<file name>`
- Import from a TFTP server
  When the file is located on a TFTP server, specify the URL for the file in the following form:
  \`tftp://<IP address>/<path>/<file name>`
- Import from an SCP or SFTP server
  When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
  \`scp://` or \`sftp://<IP address>/<path>/<file name>`

Back to factory...

Resets the settings in the device to the default values.

- The device deletes the saved configuration profiles from the volatile memory (RAM) and from the non-volatile memory (NVM).
- The device deletes the HTTPS certificate used by the web server in the device.
- The device deletes the RSA key (Host Key) used by the SSH server in the device.
- When an external memory is connected, the device deletes the configuration profiles saved in the external memory.
- After a brief period, the device reboots and loads the default values.

Back to default

Deletes the current operating (running-config) settings from the volatile memory (RAM).

Storage type

Displays the storage location of the configuration profile.

Possible values:

- **RAM** (volatile memory of the device)
  In the volatile memory, the device stores the settings for the current operation.
Basic Settings

[Basic Settings > Load/Save]

**NVM** (non-volatile memory of the device)
When applying the *Undo configuration modifications* function or during the system startup, the device loads the “Selected” configuration profile from the non-volatile memory.
The non-volatile memory provides space for multiple configuration profiles, depending on the number of settings saved in the configuration profile. The device manages a maximum of 20 configuration profiles in the non-volatile memory.
You can load a configuration profile into the volatile memory (*RAM*). To do this, perform the following steps:
- Select the table row of the configuration profile.
- Click the **button and then the *Activate* item.

**ENVM** (external memory)
In the external memory, the device saves a backup copy of the “Selected” configuration profile.
The prerequisite is that in the *Basic Settings > External Memory* dialog the *Backup config when saving* checkbox is marked.

### Profile name
Displays the name of the configuration profile.

**Possible values:**
- **running-config**
  Name of the configuration profile in the volatile memory (*RAM*).
- **config**
  Name of the factory setting configuration profile in the non-volatile memory (*NVM*).
- **User-defined name**
  The device lets you save a configuration profile with a user-specified name. To do this, select the table row of an existing configuration profile in the table, click the **button and then the Save as.. item.

To export the configuration profile as an XML file on your PC, click the link. Then you select the storage location and specify the file name.

To save the file on a remote server, click the **button and then the Export... item.

### Modification date (UTC)
Displays the time (UTC) at which a user last saved the configuration profile.

### Selected
Displays if the configuration profile is designated as “Selected”.

The device lets you designate another configuration profile as “Selected”. To do this, select the desired configuration profile in the table, click the **button and then the *Activate* item.
Possible values:

► marked
  The configuration profile is designated as “Selected”.
  – When applying the *Undo configuration modifications* function or during the system startup, the device loads the configuration profile into the volatile memory (*RAM*).
  – When you click the button, the device saves the temporarily saved settings in this configuration profile.

► unmarked
  Another configuration profile is designated as “Selected”.

**Encrypted**

Displays if the configuration profile is encrypted.

Possible values:

► marked
  The configuration profile is encrypted.

► unmarked
  The configuration profile is unencrypted.

You activate/deactivate the encryption of the configuration profile in the *Configuration encryption* frame.

**Encryption verified**

Displays if the password of the encrypted configuration profile matches the password stored in the device.

Possible values:

► marked
  The passwords match. The device is able to unencrypt the configuration profile.

► unmarked
  The passwords are different. The device is unable to unencrypt the configuration profile.

**Note:** The device applies script files additionally to the current settings. Verify that the script file does not contain any parts that conflict with the current settings.

**Software version**

Displays the version number of the device software that the device ran while saving the configuration profile.

**Fingerprint**

Displays the checksum saved in the configuration profile.

When saving the settings, the device calculates the checksum and inserts it into the configuration profile.

**Fingerprint verified**

Displays if the checksum saved in the configuration profile is valid.

The device calculates the checksum of the configuration profile marked as “Selected” and compares it with the checksum saved in this configuration profile.
Possible values:

- **marked**
  The calculated and the saved checksum match. The saved settings are consistent.

- **unmarked**
  For the configuration profile marked as “Selected” applies:
  The calculated and the saved checksum are different. The configuration profile contains modified settings.
  Possible causes:
  - The file is damaged.
  - The file system in the external memory is inconsistent.
  - A user has exported the configuration profile and changed the XML file outside the device.
  For the other configuration profiles the device has not calculated the checksum.

The device verifies the checksum correctly only if the configuration profile has been saved before as follows:
- on an identical device
- with the same software version, which the device is running
- with a lower or the same level of the device software such as HiOS-2A or HiOS-3S on a device which runs HiOS-3S

**Note:** This function identifies changes to the settings in the configuration profile. The function does not provide protection against operating the device with modified settings.
1.7 External Memory

This dialog lets you activate functions that the device automatically executes in combination with the external memory. The dialog also displays the operating state and identifying characteristics of the external memory.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Type

Displays the type of the external memory.

Possible values:

- **usb**
  - External USB memory (ACA21/ACA22)

Status

Displays the operating state of the external memory.

Possible values:

- **notPresent**
  - No external memory connected.
- **removed**
  - Someone has removed the external memory from the device during operation.
- **ok**
  - The external memory is connected and ready for operation.
- **outOfMemory**
  - The memory space is occupied in the external memory.
- **genericErr**
  - The device has detected an error.

Writable

Displays if the device has write access to the external memory.

Possible values:

- **marked**
  - The device has write access to the external memory.
- **unmarked**
  - The device has read-only access to the external memory. Possibly the write protection is activated in the external memory.
Software auto update

Activates/deactivates the automatic device software update during the system startup.

Possible values:

- **marked** (default setting)
  
  The device updates the device software when the following files are located in the external memory:
  - the image file of the device software
  - a text file `startup.txt` with the content `autoUpdate=<image_file_name>.bin`

- **unmarked**
  
  No automatic device software update during the system startup.

SSH key auto upload

Activates/deactivates the loading of the RSA key from an external memory during the system startup.

Possible values:

- **marked** (default setting)
  
  The loading of the RSA key is activated.
  
  During the system startup, the device loads the RSA key from the external memory when the following files are located in the external memory:
  - SSH RSA key file
  - a text file `startup.txt` with the content `autoUpdateRSA=<filename_of_the_SSH_RSA_key>

  The device displays messages on the system console of the serial interface.

- **unmarked**
  
  The loading of the RSA key is deactivated.

**Note:** When loading the RSA key from the external memory (ENVM), the device overwrites the existing keys in the non-volatile memory (NVM).

Config priority

Specifies the memory from which the device loads the configuration profile upon reboot.

Possible values:

- **disable**
  
  The device loads the configuration profile from the non-volatile memory (NVM).

- **first**
  
  The device loads the configuration profile from the external memory.
  
  When the device does not find a configuration profile in the external memory, it loads the configuration profile from the non-volatile memory (NVM).

**Note:** When loading the configuration profile from the external memory (ENVM), the device overwrites the settings of the Selected configuration profile in the non-volatile memory (NVM).

If the Config priority column has the value **first** and the configuration profile is unencrypted, then the Security status frame in the Basic Settings > System dialog displays an alarm.

In the Diagnostics > Status Configuration > Security Status dialog, Global tab, Monitor column you specify if the device monitors the Load unencrypted config from external memory parameter.
Backup config when saving

Activates/deactivates creating a copy of the configuration profile in the external memory.

Possible values:
- marked (default setting)
  - Creating a copy is activated. When you click in the Basic Settings > Load/Save dialog the button, the device generates a copy of the configuration profile on the active external memory.
- unmarked
  - Creating a copy is deactivated. The device does not generate a copy of the configuration profile.

Manufacturer ID

Displays the name of the memory manufacturer.

Revision

Displays the revision number specified by the memory manufacturer.

Version

Displays the version number specified by the memory manufacturer.

Name

Displays the product name specified by the memory manufacturer.

Serial number

Displays the serial number specified by the memory manufacturer.
1.8 Port

This dialog lets you specify settings for the individual ports. The dialog also displays the operating mode, connection status, bit rate and duplex mode for every port.

The dialog contains the following tabs:
- [Configuration]
- [Statistics]
- [Utilization]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Name

Name of the port.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters
  The device accepts the following characters:
  - <space>
  - 0..9
  - a..z
  - A..Z
  - !#$%&'()+,-./:;<=>?@[\]^_`{}~

Port on

Activates/deactivates the port.

Possible values:
- marked (default setting)
  The port is active.
- unmarked
  The port is inactive. The port does not send or receive any data.
State
Displays if the port is currently physically enabled or disabled.

Possible values:
- **marked**
  The port is physically enabled.
- **unmarked**
  The port is physically disabled.
When the **Port on** function is active, the **Auto-Disable** function has disabled the port.
You specify the settings of the **Auto-Disable** function in the **Diagnostics > Ports > Auto-Disable** dialog.

Power state (port off)
Specifies if the port is physically switched on or off when you deactivate the port with the **Port on** function.

Possible values:
- **marked**
  The port remains physically enabled. A connected device receives an active link.
- **unmarked** (default setting)
  The port is physically disabled.

Auto power down
Specifies how the port behaves when no cable is connected.

Possible values:
- **no-power-save** (default setting)
  The port remains activated.
- **auto-power-down**
  The port changes to the energy-saving mode.
- **unsupported**
  The port does not support this function and remains activated.

Automatic configuration
Activates/deactivates the automatic selection of the operating mode for the port.

Possible values:
- **marked** (default setting)
  The automatic selection of the operating mode is active.
The port negotiates the operating mode independently using autonegotiation and detects the devices connected to the TP port automatically (Auto Cable Crossing). This setting has priority over the manual setting of the port.
Elapse several seconds until the port has set the operating mode.
- **unmarked**
  The automatic selection of the operating mode is inactive.
The port operates with the values you specify in the **Manual configuration** column and in the **Manual cable crossing (Auto. conf. off)** column.
- Grayed-out display
  No automatic selection of the operating mode.
Manual configuration

Specifies the operating mode of the ports when the *Automatic configuration* function is disabled.

Possible values:
- 10 Mbit/s HDX
  Half duplex connection
- 10 Mbit/s FDX
  Full duplex connection
- 100 Mbit/s HDX
  Half duplex connection
- 100 Mbit/s FDX
  Full duplex connection
- 1000 Mbit/s FDX
  Full duplex connection

*Note*: The operating modes of the port actually available depend on the device hardware and the media module used.

Link/Current settings

Displays the operating mode which the port currently uses.

Possible values:
- -
  No cable connected, no link.
- 10 Mbit/s HDX
  Half duplex connection
- 10 Mbit/s FDX
  Full duplex connection
- 100 Mbit/s HDX
  Half duplex connection
- 100 Mbit/s FDX
  Full duplex connection
- 1000 Mbit/s FDX
  Full duplex connection

*Note*: The operating modes of the port actually available depend on the device hardware and the media module used.

Manual cable crossing (Auto. conf. off)

Specifies the devices connected to a TP port.

The prerequisite is that the *Automatic configuration* function is disabled.

Possible values:
- mdi
  The device interchanges the send- and receive-line pairs on the port.
- mdix (default setting on TP ports)
  The device helps prevent the interchange of the send- and receive-line pairs on the port.
### Basic Settings

**Basic Settings > Port**

- **auto-mdix**
  The device detects the send and receive line pairs of the connected device and automatically adapts to them.
  Example: When you connect an end device with a crossed cable, the device automatically resets the port from *mdix* to *mdi*.

- **unsupported** (default setting on optical ports or TP-SFP ports)
  The port does not support this function.

### Flow control

Activates/deactivates the flow control on the port.

Possible values:

- **marked** (default setting)
  The Flow control on the port is active.
  The sending and evaluating of pause packets (full-duplex operation) or collisions (half-duplex operation) is activated on the port.
  - To enable the flow control in the device, also activate the *Flow control* function in the **Switching > Global** dialog.
  - Activate the flow control also on the port of the device that is connected to this port.
  On an uplink port, activating the flow control can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”).

- **unmarked**
  The Flow control on the port is inactive.

If you are using a redundancy function, then you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

### Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status on the port.

Possible values:

- **marked** (default setting)
  The sending of SNMP traps is active. The prerequisite is that in the **Diagnostics > Status Configuration > Alarms (Traps)** dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  When the device detects a link up/down status change, the device sends an SNMP trap.

- **unmarked**
  The sending of SNMP traps is inactive.

### Signal

Activates/deactivates the port LED flashing. This function lets you identify the port in the field.

Possible values:

- **marked**
  The flashing of the port LED is active.
  The port LED flashes until you disable the function again.

- **unmarked** (default setting)
  The flashing of the port LED is inactive.
[Statistics]

This tab displays the following overview per port:

- **Number of data packets/bytes received by the device**
  - Received packets
  - Received octets
  - Received unicast packets
  - Received multicast packets
  - Received broadcast packets

- **Number of data packets/bytes sent or forwarded by the device**
  - Transmitted packets
  - Transmitted octets
  - Transmitted unicast packets
  - Transmitted multicast packets
  - Transmitted broadcast packets

- **Number of errors detected by the device**
  - Received fragments
  - Detected CRC errors
  - Detected collisions

- **Number of data packets per size category received by the device**
  - Packets 64 bytes
  - Packets 65 to 127 bytes
  - Packets 128 to 255 bytes
  - Packets 256 to 511 bytes
  - Packets 512 to 1023 bytes
  - Packets 1024 to 1518 bytes

- **Number of data packets discarded by the device**
  - Received discards
  - Transmitted discards

To sort the table by a specific criterion click the header of the corresponding column.

For example, to sort the table based on the number of received bytes in ascending order, click the header of the Received octets column once. To sort in descending order, click the header again.

To reset the counter for the port statistics in the table to 0, perform the following steps:

- In the Basic Settings > Port dialog, click the button.
- In the Basic Settings > Restart dialog, click the Clear port statistics button.

[Utilization]

This tab displays the utilization (network load) for the individual ports.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.
Basic Settings

[Basic Settings > Port]

Utilization [%]

Displays the current utilization in percent in relation to the time interval specified in the Control interval [s] column.

The utilization is the relationship of the received data quantity to the maximum possible data quantity at the currently configured data rate.

Lower threshold [%]

Specifies a lower threshold for the utilization. If the utilization of the port falls below this value, then the Alarm column displays an alarm.

Possible values:

- 0.00..100.00 (default setting: 0.00)

The value 0 deactivates the lower threshold.

Upper threshold [%]

Specifies an upper threshold for the utilization. If the utilization of the port exceeds this value, then the Alarm column displays an alarm.

Possible values:

- 0.00..100.00 (default setting: 0.00)

The value 0 deactivates the upper threshold.

Control interval [s]

Specifies the interval in seconds.

Possible values:

- 1..3600 (default setting: 30)

Alarm

Displays the utilization alarm status.

Possible values:

- marked
  
  The utilization of the port is below the value specified in the Lower threshold [%] column or above the value specified in the Upper threshold [%] column. The device sends an SNMP trap. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.

- unmarked
  
  The utilization of the port is above the value specified in the Lower threshold [%] column and below the value specified in the Upper threshold [%] column.
1.9 **Power over Ethernet**

In Power over Ethernet (PoE), the Power Source Equipment (PSE) supplies current to powered devices (PD) such as IP phones through the twisted pair cable.

The product code and the PoE-specific labeling on the PSE device housing indicates if your device supports *Power over Ethernet*. The PoE ports of the device support Power over Ethernet according to IEEE 802.3at.

The system provides an internal maximum power budget for the ports. The ports reserve power according to the detected class of a connected powered device. The real delivered power is equal to or less than the reserved power.

You manage the power output with the *Priority* parameter. When the sum of the power required by the connected devices exceeds the power available, the device turns off power supplied to the ports according to configured priority. The device turns off power supplied to the ports starting with ports configured as a low priority first. When several ports have a low priority, the device turns off power starting with the higher numbered ports.

The menu contains the following dialogs:

- PoE Global
- PoE Port
### 1.9.1 PoE Global

Based on the settings specified in this dialog, the device provides power to the end-user devices. If the power consumption reaches the user-specified threshold, then the device sends an SNMP trap.

#### Operation

**Operation**

Enables/disables the *Power over Ethernet* function.

Possible values:
- **On** (default setting)
  - The *Power over Ethernet* function is enabled.
- **Off**
  - The *Power over Ethernet* function is disabled.

#### Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Module**

Device module to which the table rows relate.

**Configured power budget [W]**

Specifies the power of the modules for the distribution at the ports.

Possible values:
- **0..n** (default setting: n)
  - Here, n corresponds to the value in the *Max. power budget [W]* column.

**Max. power budget [W]**

Displays the maximum power available for this module.

**Reserved power [W]**

Displays the power reserved for the module according to the detected classes of the connected powered devices.

**Delivered power [W]**

Displays the actual power in watts delivered to powered devices connected to this port.
Delivered current [mA]

Displays the actual current in milliamperes delivered to powered devices connected to this port.

Power source

Displays the power sourcing equipment for the device.

Possible values:
- **internal**
  - Internal power source
- **external**
  - External power source

Threshold [%]

Specifies the threshold value for the power consumption of the module in percent. If the power output exceeds this threshold, then the device measures the total output power and sends an SNMP trap.

Possible values:
- **0..99** (default setting: 90)

Send trap

Activates/deactivates the sending of SNMP traps if the device detects that the threshold value for the power consumption exceeds.

Possible values:
- **marked**
  - The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
  - If the power consumption of the module exceeds the user-defined threshold, then the device sends an SNMP trap.
- **unmarked** (default setting)
  - The sending of SNMP traps is inactive.
1.9.2 PoE Port

When power consumption is higher than deliverable power, the device turns off power to the powered devices (PD) according to the priority levels and port numbers. When the PDs connected require more power than the device provides, the device deactivates the Power over Ethernet function on the ports. The device disables the Power over Ethernet function on the ports with the lowest priority first. When multiple ports have the same priority, the device first disables the Power over Ethernet function on the ports with the higher port number. The device also turns off power to powered devices (PD) for a specified time period.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE enable</td>
<td>Activates/deactivates the PoE power provided to the port.</td>
</tr>
<tr>
<td>Fast startup</td>
<td>Activates/deactivates the Power over Ethernet Fast Startup function on the port.</td>
</tr>
</tbody>
</table>

**Fast startup**

Activates/deactivates the Power over Ethernet Fast Startup function on the port.

The prerequisite is that the checkbox in the PoE enable column is marked.

Possible values:

- **marked** (default setting)
  - The fast start up function is active. The device sends power to the powered devices (PD) immediately after turning the power to the device on.

- **unmarked** (default setting)
  - The fast start up function is inactive. The device sends power to the powered devices (PD) after loading its own configuration.
Priority

Specifies the port priority.

To help prevent current overloads, the device disables ports with low priority first. To help prevent that the device disables the ports supplying necessary devices, specify a high priority for these ports.

Possible values:
- `critical`
- `high`
- `low` (default setting)

Status

Displays the status of the port Powered Device (PD) detection.

Possible values:
- `disabled`
  The device is in the DISABLED state and is not delivering power to the powered devices.
- `deliveringPower`
  The device identified the class of the connected PD and is in the POWER ON state.
- `fault`
  The device is in the TEST ERROR state.
- `otherFault`
  The device is in the IDLE state.
- `searching`
  The device is in a state other than the listed states.
- `test`
  The device is in the TEST MODE.

Detected class

Displays the power class of the powered device connected to the port.

Possible values:
- `Class 0`
- `Class 1`
- `Class 2`
- `Class 3`
- `Class 4`

Activates/deactivates the current of the classes 0 to 4 on the port.

Possible values:
- `marked` (default setting)
- `unmarked`
Consumption [W]

Displays the current power consumption of the port in watts.

Possible values:

- \(0,0\ldots30,0\)

Consumption [mA]

Displays the current delivered to the port in milliamperes.

Possible values:

- \(0\ldots600\)

Power limit [W]

Specifies the maximum power in watts that the port outputs.

This function lets you distribute the power budget available among the PoE ports as required.

For example, for a connected device not providing a “Power Class”, the port reserves a fixed amount of 15.4 W (class 0) even if the device requires less power. The surplus power is not available to any other port.

By specifying the power limit, you reduce the reserved power to the actual requirement of the connected device. The unused power is available to other ports.

If the exact power consumption of the connected powered device is unknown, then the device displays the value in the Max. consumption [W] column. Verify that the power limit is greater than the value in the Max. consumption [W] column.

If the maximum observed power is greater than the set power limit, then the device sees the power limit as invalid. In this case, the device uses the PoE class for the calculation.

Possible values:

- \(0,0\ldots30,0\) (default setting: 0)

Max. consumption [W]

Displays the maximum power in watts that the device has consumed so far.

You reset the value when you disable PoE on the port or terminate the connection to the connected device.

Name

Specifies the name of the port.

Specify the name of your choice.
Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Auto-shutdown power

Activates/deactivates the Auto-shutdown power function according to the settings.

Possible values:

- marked
- unmarked (default setting)

Disable power at [hh:mm]

Specifies the time at which the device disables the power for the port upon activation of the Auto-shutdown power function.

Possible values:

- 00:00..23:59 (default setting: 00:00)

Re-enable power at [hh:mm]

Specifies the time at which the device enables the power for the port upon activation of the Auto-shutdown power function.

Possible values:

- 00:00..23:59 (default setting: 00:00)

### 1.10 Restart

Restart

This dialog lets you restart the device, reset port counters and address tables, and delete log files.

**Restart**

**Restart in**

Displays the remaining time in days, hours, minutes, seconds until the device restarts.

To update the display of the remaining time, click the ⌚ button.

**Cancel**

Aborts a delayed restart.
Cold start...

Opens the Restart window to initiate an immediate or delayed restart of the device.

If the configuration profile in the volatile memory (RAM) and the "Selected" configuration profile in the non-volatile memory (NVM) differ, then the device displays the Warning window.

- To permanently save the settings, click the Yes button in the Warning window.
- To discard the changed settings, click the No button in the Warning window.
- In the Restart in field you specify the delay time for the delayed restart.
  Possible values:
  - 00:00:00..596:31:23 (default setting: 00:00:00) Hour:Minute:Second

When the delay time elapsed, the device restarts and goes through the following phases:
- If you activate the function in the Diagnostics > System > Selftest dialog, then the device performs a RAM test.
- The device starts the device software that the Stored version field displays in the Basic Settings > Software dialog.
- The device loads the settings from the "Selected" configuration profile. See the Basic Settings > Load/Save dialog.

Note: During the restart, the device does not transfer any data. During this time, the device cannot be accessed by the Graphical User Interface or other management systems.

Buttons

Reset MAC address table

Removes the MAC addresses from the forwarding table that have in the Switching > Filter for MAC Addresses dialog the value learned in the Status column.

Reset ARP table

Removes the dynamically set up addresses from the ARP table.

See the Diagnostics > System > ARP dialog.

Clear port statistics

Resets the counter for the port statistics to 0.

See the Basic Settings > Port dialog, Statistics tab.

Clear management access statistics

Resets the counters for statistics on device management access to 0.

See the Diagnostics > System > System Information dialog, Used Management Ports table.
Basic Settings

[Basic Settings > Restart]

Reset IGMP snooping data

Removes the IGMP Snooping entries and resets the counter in the Information frame to 0.

See the Switching > IGMP Snooping > Global dialog.

Delete log file

Removes the logged events from the log file.

See the Diagnostics > Report > System Log dialog.

Delete persistent log file

Removes the log files from the external memory.

See the Diagnostics > Report > Persistent Logging dialog.

Clear email notification statistics

Resets the counters in the Information frame to 0.

See the Diagnostics > Email Notification > Global dialog.
2 Time

The menu contains the following dialogs:
- Basic Settings
- SNTP

2.1 Basic Settings

The device is equipped with a buffered hardware clock. This clock maintains the correct time if the power supply becomes inoperable or you disconnect the device from the power supply. After the device is started, the current time is available to you, for example for log entries.

The hardware clock bridges a power supply downtime of 3 hours. The prerequisite is that the power supply of the device has been connected continually for at least 5 minutes beforehand.

In this dialog you specify time-related settings independently of the time synchronization protocol specified.

The dialog contains the following tabs:
- [Global]
- [Daylight saving time]

[Global]

In this tab you specify the system time in the device and the time zone.

Configuration

System time (UTC)

Displays the current date and time with reference to Universal Time Coordinated (UTC).

Set time from PC

The device uses the time on the PC as the system time.

System time

Displays the current date and time with reference to the local time: $\text{System time} = \text{System time (UTC)} + \text{Local offset [min]} + \text{Daylight saving time}$

Time source

Displays the time source from which the device gets the time information.

The device automatically selects the available time source with the greatest accuracy.
Possible values:

- **local**
  System clock of the device.

- **sntp**
  The SNTP client is enabled and the device is synchronized by an SNTP server.

**Local offset [min]**

Specifies the difference between the local time and System time (UTC) in minutes: Local offset [min] = System time − System time (UTC)

Possible values:

- **-780..840** (default setting: 60)

**[Daylight saving time]**

In this tab you activate the automatic daylight saving time function. You specify the beginning and the end of summertime using a pre-defined profile, or you specify these settings individually. During summertime, the device puts the local time forward by 1 hour.

**Operation**

**Daylight saving time**

Enables/disables the Daylight saving time mode.

Possible values:

- **On**
  The Daylight saving time mode is enabled.
  The device automatically changes between summertime and wintertime.

- **Off** (default setting)
  The Daylight saving time mode is disabled.

The times at which the device changes between summertime and wintertime are specified in the Summertime begin and Summertime end frames.

**Profile...**

Opens the Profile... window to select a pre-defined profile for the beginning and the end of summertime. This profile overwrites the settings in the Summertime begin and Summertime end frames.

**Summertime begin**

In the first 3 fields you specify the day for the beginning of summertime, and in the last field the time.

When the time in the System time field reaches the value entered here, the device switches to summertime.
Week

Specifies the week in the current month.

Possible values:
- (default setting)
  - first
  - second
  - third
  - fourth
  - last

Day

Specifies the day of the week.

Possible values:
- (default setting)
  - Sunday
  - Monday
  - Tuesday
  - Wednesday
  - Thursday
  - Friday
  - Saturday

Month

Specifies the month.

Possible values:
- (default setting)
  - January
  - February
  - March
  - April
  - May
  - June
  - July
  - August
  - September
  - October
  - November
  - December
System time

Specifies the time.

Possible values:

► <HH:MM>  (default setting: 00:00)

Summertime end

In the first 3 fields you specify the day for the end of summertime, and in the last field the time.

When the time in the System time field reaches the value entered here, the device switches to wintertime.

Week

Specifies the week in the current month.

Possible values:

► -  (default setting)
► first
► second
► third
► fourth
► last

Day

Specifies the day of the week.

Possible values:

► -  (default setting)
► Sunday
► Monday
► Tuesday
► Wednesday
► Thursday
► Friday
► Saturday

Month

Specifies the month.

Possible values:

► -  (default setting)
► January
► February
► March
► April
2.2 SNTP

The Simple Network Time Protocol (SNTP) is a procedure described in the RFC 4330 for time synchronization in the network.

The device lets you synchronize the system time in the device as an SNTP client. As the SNTP server, the device makes the time information available to other devices.

The menu contains the following dialogs:
- SNTP Client
- SNTP Server
2.2.1 SNTP Client

In this dialog you specify the settings with which the device operates as an SNTP client.

As an SNTP client the device obtains the time information from both SNTP servers and NTP servers and synchronizes the local clock with the time of the time server.

Operation

Enables/disables the Client function of the device.

Possible values:
- **On** (default setting)
  The Client function is enabled.
  The device operates as an SNTP client.
- **Off**
  The Client function is disabled.

State

Displays the status of the SNTP client.

Possible values:
- **disabled**
  The SNTP client is disabled.
- **notSynchronized**
  The SNTP client is not synchronized with any SNTP or NTP server.
- **synchronizedToRemoteServer**
  The SNTP client is synchronized with an SNTP or NTP server.
Configuration

Mode

Specifies if the device actively requests the time information from an SNTP server known and configured in the network (Unicast mode) or passively waits for the time information from a random SNTP server (Broadcast mode).

Possible values:
- **unicast** (default setting)
  The device takes the time information only from the configured SNTP server. The device sends Unicast requests to the SNTP server and evaluates its responses.
- **broadcast**
  The device obtains the time information from one or more SNTP or NTP servers. The device evaluates the Broadcasts or Multicasts only from these servers.

Request interval [s]

Specifies the interval in seconds at which the device requests time information from the SNTP server.

Possible values:
- **5..3600** (default setting: 30)

Broadcast recv timeout [s]

Specifies the time in seconds a client in broadcast client mode waits before changing the value in the field from *syncToRemoteServer* to *notSynchronized* when the client receives no broadcast packets.

Possible values:
- **128..2048** (default setting: 320)

Disable client after successful sync

Activates/deactivates the disabling of the SNTP client after the device has successfully synchronized the time.

Possible values:
- **marked**
  The disabling of the SNTP client is active. The device deactivates the SNTP client after successful time synchronization.
- **unmarked** (default setting)
  The disabling of the SNTP client is inactive. The SNTP client remains active after successful time synchronization.

Table

In the table you specify the settings for up to 4 SNTP servers.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.
Time
[Time > SNTP > Client]

Buttons

Add
Adds a table row.

Remove
Removes the selected table row.

Index
Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

When you delete a table row, this leaves a gap in the numbering. When you create a new table row, the device fills the first gap.

After starting, the device sends requests to the SNTP server configured in the first table row. When the server does not reply, the device sends its requests to the SNTP server configured in the next table row.

If none of the configured SNTP servers responds in the meantime, then the SNTP client interrupts its synchronization. The device cyclically sends requests to each SNTP server until a server delivers a valid time. The device synchronizes itself with this SNTP server, even if the other servers can be reached again later.

Name
Specifies the name of the SNTP server.
Possible values:
▶ Alphanumeric ASCII character string with 1..32 characters

Address
Specifies the IP address of the SNTP server.
Possible values:
▶ Valid IPv4 address (default setting: 0.0.0.0)
▶ Valid IPv6 address
▶ Hostname

Destination UDP port
Specifies the UDP Port on which the SNTP server expects the time information.
Possible values:
▶ 1..65535 (default setting: 123)
   Exception: Port 2222 is reserved for internal functions.
Status

Displays the connection status between the SNTP client and the SNTP server.

Possible values:

- **success**
  
The device has successfully synchronized the time with the SNTP server.

- **badDateEncoded**
  
The time information received contains protocol errors - synchronization was unsuccessful.

- **other**
  
  - The value 0.0.0.0 is entered for the IP address of the SNTP server - synchronization did not succeed.
  
  or
  
  - The SNTP client is using a different SNTP server.

- **requestTimedOut**
  
The device has not received a reply from the SNTP server - synchronization was unsuccessful.

- **serverKissOfDeath**
  
The SNTP server is overloaded. The device is requested to synchronize itself with another SNTP server. When no other SNTP server is available, the device checks at intervals longer than the setting in the Request interval [s] field, if the server is still overloaded.

- **serverUnsynchronized**
  
The SNTP server is not synchronized with either a local or an external reference time source - synchronization was unsuccessful.

- **versionNotSupported**
  
The SNTP versions on the client and the server are incompatible with each other - synchronization was unsuccessful.

Active

Activates/deactivates the connection to the SNTP server.

Possible values:

- **marked**
  
The connection to the SNTP server is activated.
  
The SNTP client has access to the SNTP server.

- **unmarked** (default setting)
  
The connection to the SNTP server is deactivated.
  
The SNTP client has no access to the SNTP server.
2.2.2 **SNTP Server**

In this dialog you specify the settings with which the device operates as an **SNTP** server.

The **SNTP** server provides the Universal Time Coordinated (UTC) without considering local time differences.

If the setting is appropriate, then the **SNTP** server operates in the broadcast mode. In broadcast mode, the **SNTP** server automatically sends broadcast messages or multicast messages according to the broadcast send interval.

**Operation**

Enables/disables the **Server** function of the device.

Possible values:

- **On**
  - The **Server** function is enabled.
  - The device operates as an **SNTP** server.

- **Off** (default setting)
  - The **Server** function is disabled.

Note the setting in the **Disable server at local time source** checkbox in the **Configuration** frame.

**State**

Displays the state of the **SNTP** server.

Possible values:

- **disabled**
  - The **SNTP** server is disabled.

- **notSynchronized**
  - The **SNTP** server is not synchronized with either a local or an external reference time source.

- **syncToLocal**
  - The **SNTP** server is synchronized with the hardware clock of the device.

- **syncToRefclock**
  - The **SNTP** server is synchronized with an external reference time source.

- **syncToRemoteServer**
  - The **SNTP** server is synchronized with an **SNTP** server that is higher than the device in a cascade.
**Configuration**

**UDP port**

Specifies the number of the UDP port on which the **SNTP** server of the device receives requests from other clients.

Possible values:
- 1..65535 (default setting: 123)

Exception: Port 2222 is reserved for internal functions.

**Broadcast admin mode**

Activates/deactivates the Broadcast mode.

- marked
  
  The **SNTP** server replies to requests from **SNTP** clients in Unicast mode and also sends **SNTP** packets in Broadcast mode as Broadcasts or Multicasts.

- unmarked (default setting)
  
  The **SNTP** server replies to requests from **SNTP** clients in the Unicast mode.

**Broadcast destination address**

Specifies the IP address to which the **SNTP** server of the device sends the **SNTP** packets in Broadcast mode.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Broadcast and Multicast addresses are permitted.

**Broadcast UDP port**

Specifies the number of the UDP port on which the **SNTP** server sends the **SNTP** packets in Broadcast mode.

Possible values:
- 1..65535 (default setting: 123)

Exception: Port 2222 is reserved for internal functions.

**Broadcast VLAN ID**

Specifies the ID of the VLAN in which the **SNTP** server of the device sends the **SNTP** packets in Broadcast mode.

Possible values:
- 0

The **SNTP** server sends the **SNTP** packets in the same VLAN in which the access to the device management is possible. See the **Basic Settings > Network > Global** dialog.

- 1..4042 (default setting: 1)
Broadcast send interval [s]

Specifies the time interval at which the **SNTP** server of the device sends **SNTP** broadcast packets.

Possible values:

- **64..1024** (default setting: **128**)

Disable server at local time source

Activates/deactivates the disabling of the **SNTP** server when the device is synchronized to the local clock.

Possible values:

- **marked**
  The disabling of the **SNTP** server is active.
  If the device is synchronized to the local clock, then the device disables the **SNTP** server. The **SNTP** server continues to reply to requests from **SNTP** clients. In the **SNTP** packet, the **SNTP** server informs the clients that it is synchronized locally.

- **unmarked** (default setting)
  The disabling of the **SNTP** server is inactive.
  If the device is synchronized to the local clock, then the **SNTP** server remains active.
3 Device Security

The menu contains the following dialogs:
- User Management
- Authentication List
- LDAP
- Management Access
- Pre-login Banner

3.1 User Management

If users log in with valid login data, then the device lets them have access to its device management.

In this dialog you manage the users of the local user management. You also specify the following settings here:
- Settings for the login
- Settings for saving the passwords
- Specify policy for valid passwords

The methods that the device uses for the authentication you specify in the Device Security > Authentication List dialog.

Configuration

This frame lets you specify settings for the login.

Login attempts

Specifies the number of login attempts possible when the user accesses the device management using the Graphical User Interface and the Command Line Interface.

Note: When accessing the device management using the Command Line Interface through the serial connection, the number of login attempts is unlimited.

Possible values:
- 0..5 (default setting: 0)

If the user makes one more unsuccessful login attempt, then the device locks access for the user.

The device lets only users with the administrator authorization remove the lock.

The value 0 deactivates the lock. The user has unlimited attempts to log in.
Min. password length

The device accepts the password if it contains at least the number of characters specified here.

The device checks the password according to this setting, regardless of the setting for the Policy check checkbox.

Possible values:

- 1..64  (default setting: 6)

Login attempts period (min.)

Displays the time period before the device resets the counter in the Login attempts field.

Possible values:

- 0..60  (default setting: 0)

**Password policy**

This frame lets you specify the policy for valid passwords. The device checks every new password and password change according to this policy.

The settings effect the Password column. The prerequisite is that the checkbox in the Policy check column is marked.

Upper-case characters (min.)

The device accepts the password if it contains at least as many upper-case letters as specified here.

Possible values:

- 0..16  (default setting: 1)

The value 0 deactivates this setting.

Lower-case characters (min.)

The device accepts the password if it contains at least as many lower-case letters as specified here.

Possible values:

- 0..16  (default setting: 1)

The value 0 deactivates this setting.

Digits (min.)

The device accepts the password if it contains at least as many numbers as specified here.

Possible values:

- 0..16  (default setting: 1)

The value 0 deactivates this setting.
Special characters (min.)

The device accepts the password if it contains at least as many special characters as specified here.

Possible values:
- \(0..16\) (default setting: 1)

The value 0 deactivates this setting.

Table

Every user requires an active user account to gain access to the device management. The table lets you set up and manage user accounts. To change settings, click the desired parameter in the table and modify the value.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the Create window to add a table row.
- In the User name field, you specify the name of the user account.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters

Remove

Removes the selected table row.

User name

Displays the name of the user account.

To create a new user account, click the Add button.

Active

Activates/deactivates the user account.

Possible values:
- **marked**
  The user account is active. The device accepts the login of a user with this user name.
- **unmarked** (default setting)
  The user account is inactive. The device rejects the login of a user with this user name.

When one user account exists with the access role administrator, this user account is constantly active.
Device Security

[Device Security > User Management]

Password

Specifies the password that the user applies to access the device management using the Graphical User Interface or Command Line Interface.

Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.

When you specify the password for the first time, the device uses the same password in the SNMP auth password and SNMP encryption password columns.

• The device lets you specify different passwords in the SNMP auth password and SNMP encryption password columns.

• If you change the password in the current column, then the device also changes the passwords for the SNMP auth password and SNMP encryption password columns, but only if they are not individually specified previously.

Possible values:

► Alphanumeric ASCII character string with 6..64 characters
  The device accepts the following characters:
  – a..z
  – A..Z
  – 0..9
  – !#$%&'()*+,-./:;<=>?@[\]^_`{}~

The minimum length of the password is specified in the Configuration frame. The device differentiates between upper and lower case.

If the checkbox in the Policy check column is marked, then the device checks the password according to the policy specified in the Password policy frame.

The device constantly checks the minimum length of the password, even if the checkbox in the Policy check column is unmarked.

Role

Specifies the access role that regulates the access of the user to the individual functions of the device.

Possible values:

► unauthorized
  The user is blocked, and the device rejects the user login.
  Assign this value to temporarily lock the user account. If the device detects an error when another access role is being assigned, then the device assigns this access role to the user account.

► guest (default setting)
  The user is authorized to monitor the device.

► auditor
  The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog.

► operator
  The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access.

► administrator
  The user is authorized to monitor the device and to change the settings.
The device assigns the Service Type transferred in the response of a RADIUS server as follows to an access role:

- **Administrative-User**: administrator
- **Login-User**: operator
- **NAS-Prompt-User**: guest

### User locked

Unlocks the user account.

**Possible values:**

- **marked**: The user account is locked. The user has no access to the device management.
  - If the user makes too many unsuccessful login attempts, then the device automatically locks the user.
- **unmarked** (grayed out) (default setting): The user account is unlocked. The user has access to the device management.

### Policy check

Activates/deactivates the password check.

**Possible values:**

- **marked**: The password check is activated.
  - When you set up or change the password, the device checks the password according to the policy specified in the Password policy frame.
- **unmarked** (default setting): The password check is deactivated.

### SNMP auth type

Specifies the authentication protocol that the device applies for user access using SNMPv3.

**Possible values:**

- **hmacmd5** (default value): For this user account, the device uses protocol HMACMD5.
- **hmacsha**: For this user account, the device uses protocol HMACSHA.

### SNMP auth password

Specifies the password that the device applies for user access using SNMPv3.

Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.

By default, the device uses the same password that you specify in the Password column.

- For the current column, the device lets you specify a different password than in the Password column.
- If you change the password in the Password column, then the device also changes the password for the current column, but only if it is not individually specified.
Possible values:

- **Alphanumeric ASCII character string with 6..64 characters**  
The device accepts the following characters:
  - a..z
  - A..Z
  - 0..9
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

**SNMP encryption type**

Specifies the encryption protocol that the device applies for user access using SNMPv3.

Possible values:

- **none**  
  No encryption.
- **des** (default value)  
  DES encryption
- **aesCfb128**  
  AES128 encryption

**SNMP encryption password**

Specifies the password that the device applies to encrypt user access using SNMPv3.

Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.

By default, the device uses the same password that you specify in the **Password** column.

- For the current column, the device lets you specify a different password than in the **Password** column.
- If you change the password in the **Password** column, then the device also changes the password for the current column, but only if it is not individually specified.

Possible values:

- **Alphanumeric ASCII character string with 6..64 characters**  
The device accepts the following characters:
  - a..z
  - A..Z
  - 0..9
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~
3.2 Authentication List

In this dialog you manage the authentication lists. In an authentication list you specify which method the device uses for the authentication. You also have the option to assign pre-defined applications to the authentication lists.

If users log in with valid login data, then the device lets them have access to its device management. The device authenticates the users using the following methods:

- User management of the device
- LDAP
- RADIUS

With the port-based access control according to IEEE 802.1X, if connected end devices log in with valid login data, then the device lets them have access to the network. The device authenticates the end devices using the following methods:

- RADIUS
- IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:

- defaultDot1x8021AuthList
- defaultLoginAuthList
- defaultV24AuthList

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Note: If the table does not contain a list, then the access to the device management is only possible using the Command Line Interface through the serial interface of the device. In this case, the device authenticates the user by using the local user management. See the Device Security > User Management dialog.

Buttons

Add

Opens the Create window to add a table row.

In the Name field, you specify the name of the list.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters
Remove

Removes the selected table row.

Allocate applications

Opens the Allocate applications window. The window displays the applications that you can designate to the selected list.

☐ Click and select an entry to designate it to the currently selected list.
   An application that is already designated to a different list the device designates to the currently selected list, after you click the Ok button.

☐ Click and deselect an entry to undo its designation to the currently selected list.
   If you deselect the application WebInterface, then the connection to the device is lost, after you click the Ok button.

Name

Displays the name of the list.

To create a new list, click the button.

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

Specifies the authentication policy that the device uses for access using the application specified in the Dedicated applications column.

The device gives you the option of a fall-back solution. For this, you specify another policy in each of the policy fields. If the authentication with the specified policy is unsuccessful, then the device can use the next policy, depending on the order of the values entered in each policy.

Possible values:

► local (default setting)
   The device authenticates the users by using the local user management. See the Device Security > User Management dialog.
   You cannot assign this value to the authentication list defaultDot1x8021AuthList.

► radius
   The device authenticates the users with a RADIUS server in the network. You specify the RADIUS server in the Network Security > RADIUS > Authentication Server dialog.
Device Security

[Device Security > Authentication List]

- **reject**
  - The device accepts or rejects the authentication depending on which policy you try first. The following list contains authentication scenarios:
    - If the first policy in the authentication list is `local` and the device accepts the login credentials of the user, then it logs the user in without attempting the other policies.
    - If the first policy in the authentication list is `local` and the device denies the login credentials of the user, then it attempts to log the user in using the other policies in the order specified.
    - If the first policy in the authentication list is `radius` or `ldap` and the device rejects a login, then the login is immediately rejected without attempting to log in the user using another policy.
    - If there is no response from the RADIUS or LDAP server, then the device attempts to authenticate the user with the next policy.
    - If the first policy in the authentication list is `reject`, then the devices immediately rejects the user login without attempting another policy.
    - Verify that the authentication list `defaultV24AuthList` contains at least one policy different from `reject`.

- **ias**
  - The device authenticates the end devices logging in using 802.1X with the integrated authentication server (IAS). The integrated authentication server manages the login data in a separate database. See the Network Security > 802.1X > Integrated Authentication Server dialog.
  - You can only assign this value to the authentication list `defaultDot1x8021AuthList`.

- **ldap**
  - The device authenticates the users with authentication data and access role saved in a central location. You specify the Active Directory server that the device uses in the Device Security > LDAP > Configuration dialog.

**Dedicated applications**

- Displays the dedicated applications. When users access the device with the relevant application, the device uses the specified policies for the authentication.

- To allocate another application to the list or remove the allocation, click the button. The device lets you assign each application to exactly one list.

**Active**

- Activates/deactivates the list.

  **Possible values:**
  - **marked** (default setting)
    - The list is activated. The device uses the policies in this list when users access the device with the relevant application.
  - **unmarked**
    - The list is deactivated.
3.3 LDAP

The Lightweight Directory Access Protocol (LDAP) lets you authenticate and authorize the users at a central point in the network. A widely used directory service accessible through LDAP is Active Directory®.

The device forwards the login data of the user to the authentication server using the LDAP protocol. The authentication server decides if the login data is valid and transfers the authorizations of the user to the device.

Upon successful login, the device saves the login data temporarily in the cache. This speeds up the login process when users log in again. In this case, no complex LDAP search operation is necessary.

The menu contains the following dialogs:
- LDAP Configuration
- LDAP Role Mapping
3.3.1 LDAP Configuration

This dialog lets you specify up to 4 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the first authentication server. When no response comes from this server, the device contacts the next server in the table.

Operation

Enables/disables the LDAP client.

If in the Device Security > Authentication List dialog you specify the value ldap in one of the columns Policy 1 to Policy 5, then the device uses the LDAP client. Prior to this, specify in the Device Security > LDAP > Role Mapping dialog at least one mapping for this access role administrator. This provides you access to the device as administrator after logging in through LDAP.

Possible values:

- **On**
  - The LDAP client is enabled.
- **Off** (default setting)
  - The LDAP client is disabled.

Configuration

Buttons

Flush cache

Removes the cached login data of the successfully logged in users.
Client cache timeout [min]

Specifies for how many minutes after successfully logging in the login data of a user remain valid. When a user logs in again within this time, no complex LDAP search operation is necessary. The login process is much faster.

Possible values:

- 1..1440 (default setting: 10)

Bind user

Specifies the user ID in the form of the “Distinguished Name” (DN) with which the device logs in to the LDAP server.

If the LDAP server requires a user ID in the form of the “Distinguished Name” (DN) for the login, then this information is necessary. In Active Directory environments, this information is unnecessary.

The device logs in to the LDAP server with the user ID to find the “Distinguished Name” (DN) for the users logging in. The device conducts the search according to the settings in the Base DN and User name attribute fields.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Bind user password

Specifies the password which the device uses together with the user ID specified in the Bind user field when logging in to the LDAP server.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

Base DN

Specifies the starting point for the search in the directory tree in the form of the “Distinguished Name” (DN).

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

User name attribute

Specifies the LDAP attribute which contains a biunique user name. Afterwards, the user uses the user name contained in this attribute to log in.

Often the LDAP attributes userPrincipalName, mail, sAMAccountName and uid contain a unique user name.

The device adds the character string specified in the Default domain field to the user name under the following condition:

- The user name contained in the attribute does not contain the @ character.
- In the Default domain field, a domain name is specified.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters (default setting: userPrincipalName)
Default domain

Specifies the character string which the device adds to the user name of the users logging in if the user name does not contain the @ character.

Possible values:
- Alphanumeric ASCII character string with 0..64 characters

CA certificate

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:
- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
  ------BEGIN CERTIFICATE------
  and
  ------END CERTIFICATE------

For security reasons, we recommend to constantly use a certificate which is signed by a certification authority.

The device gives you the following options for copying the certificate to the device:
- Import from the PC
  When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
- Import from a FTP server
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>
- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  tftp://<IP address>/<path>/<file name>
- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, specify the URL for the file in the following form:
  - scp:// or sftp://<IP address>/<path>/<file name>
  When you click the Start button, the device displays the Credentials window. There you enter User name and Password, to log in to the server.
  - scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>

Start

Copies the certificate specified in the URL field to the device.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Description

Specifies the description.

You have the option to describe here the authentication server or note additional information.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Address

Specifies the IP address or the DNS name of the server.

Possible values:

- IPv4 address (default setting: 0.0.0.0)
- IPv6 address
- DNS name in the format <domain>.<tld> or <host>.<domain>.<tld>
- _ldap._tcp.<domain>.<tld>
  Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.

If in the Connection security column a value other than none is specified and the certificate contains only DNS names of the server, then use a DNS name. Enable the Client function in the Advanced > DNS > Client > Global dialog.

Destination TCP port

Specifies the TCP Port on which the server expects the requests.

If you have specified the value _ldap._tcp.domain.tld in the Address column, then the device ignores this value.
Possible values:

- **0..65535** (default setting: 389)
  Exception: Port \textit{2222} is reserved for internal functions.

Frequently used TCP-Ports:

- **LDAP**: 389
- **LDAP over SSL**: 636
- **Active Directory Global Catalogue**: 3268
- **Active Directory Global Catalogue SSL**: 3269

**Connection security**

Specifies the protocol which encrypts the communication between the device and the authentication server.

Possible values:

- **none**
  No encryption.
  The device establishes an LDAP connection to the server and transmits the communication including the passwords in clear text.

- **ssl**
  Encryption with SSL.
  The device establishes a TLS connection to the server and tunnels the LDAP communication over it.

- **startTLS** (default setting)
  Encryption with startTLS extension.
  The device establishes an LDAP connection to the server and encrypts the communication.

The prerequisite for encrypted communication is that the device uses the correct time. If the certificate contains only the DNS names, then you specify the DNS name of the server in the Address column. Enable the Client function in the Advanced > DNS > Client > Global dialog.

If the certificate contains the IP address of the server in the “Subject Alternative Name” field, then the device is able to verify the identity of the server without the DNS configuration.

**Server status**

Displays the connection status and the authentication with the authentication server.

Possible values:

- **ok**
  The server is reachable.
  If in the Connection security column a value other than none is specified, then the device has verified the certificate of the server.

- **unreachable**
  Server is unreachable.

- **other**
  The device has not established a connection to the server yet.
Active

Activates/deactivates the use of the server.

Possible values:

- **marked**
  The device uses the server.

- **unmarked** (default setting)
  The device does not use the server.
3.3.2 LDAP Role Mapping

This dialog lets you create up to 64 mappings to assign an access role to users.

In the table you specify if the device assigns an access role to the user based on an attribute with a specific value or based on the group membership.

- The device searches for the attribute and the attribute value within the user object.
- By evaluating the “Distinguished Name” (DN) contained in the member attributes, the device checks group the membership.

When a user logs in, the device searches for the following information on the LDAP server:

- In the related user project, the device searches for attributes specified in the mappings.
- In the group objects of the groups specified in the mappings, the device searches for the member attributes.

On this basis, the device checks any mapping.
- Does the user object contain the required attribute? or
- Is the user member of the group?

If the device does not find a match, then the user does not get access to the device.

If the device finds more than one mapping that applies to a user, then the setting in the Matching policy field decides. The user either obtains the access role with the more extensive authorizations or the 1st access role in the table that applies.

Configuration

Matching policy

Specifies which access role the device applies if more than one mapping applies to a user.

Possible values:

- **highest** (default setting)
  The device applies the access role with more extensive authorizations.

- **first**
  The device applies the rule which has the lower value in the Index column to the user.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the Create window to add a table row.

- In the Index field, you specify the index number. Possible values:
  - 1..64

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. You specify the index number when you add a table row.

Role

Specifies the access role that regulates the access of the user to the individual functions of the device.

Possible values:

- unauthorized
  - The user is blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If an error is detected when another role is being assigned, then the device assigns this access role to the user account.
- guest (default setting)
  - The user is authorized to monitor the device.
- auditor
  - The user is authorized to monitor the device and to save the log file in the Diagnostics > Report > Audit Trail dialog.
- operator
  - The user is authorized to monitor the device and to change the settings – with the exception of security settings for device access.
- administrator
  - The user is authorized to monitor the device and to change the settings.

Type

Specifies if a group or an attribute with an attribute value is specified in the Parameter column.

Possible values:

- attribute (default setting)
  - The Parameter column contains an attribute with an attribute value.
- group
  - The Parameter column contains the “Distinguished Name” (DN) of a group.
Parameter

Specifies a group or an attribute with an attribute value, depending on the setting in the Type column.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  - The device differentiates between upper and lower case.
  - If in the Type column the value attribute is specified, then you specify the attribute in the form of `Attribute_name=Attribute_value`.
    - Example: `l=Germany`
  - If in the Type column the value group is specified, then you specify the “Distinguished Name” (DN) of a group.
    - Example: `CN=admin-users,OU=Groups,DC=example,DC=com`

Active

Activates/deactivates the role mapping.

Possible values:

- marked (default setting)
  - The role mapping is active.
- unmarked
  - The role mapping is inactive.

3.4 Management Access

The menu contains the following dialogs:

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community
3.4.1 Server

This dialog lets you set up the server services which enable users or applications to access the management of the device.

The dialog contains the following tabs:
- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

This tab displays as an overview which server services are enabled.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

SNMPv1

Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 1. See the SNMP tab.

Possible values:
- **marked**
  Server service is active.
- **unmarked**
  Server service is inactive.

SNMPv2

Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 2. See the SNMP tab.

Possible values:
- **marked**
  Server service is active.
- **unmarked**
  Server service is inactive.
SNMPv3
Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 3. See the SNMP tab.

Possible values:
- **marked**
  - Server service is active.
- **unmarked**
  - Server service is inactive.

Telnet server
Displays if the server service is active or inactive, which authorizes access to the device using Telnet. See the Telnet tab.

Possible values:
- **marked**
  - Server service is active.
- **unmarked**
  - Server service is inactive.

SSH server
Displays if the server service is active or inactive, which authorizes access to the device using Secure Shell. See the SSH tab.

Possible values:
- **marked**
  - Server service is active.
- **unmarked**
  - Server service is inactive.

HTTP server
Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTP. See the HTTP tab.

Possible values:
- **marked**
  - Server service is active.
- **unmarked**
  - Server service is inactive.

HTTPS server
Displays if the server service is active or inactive, which authorizes access to the device using the Graphical User Interface through HTTPS. See the HTTPS tab.

Possible values:
- **marked**
  - Server service is active.
- **unmarked**
  - Server service is inactive.
[SNMP]

This tab lets you specify settings for the SNMP agent of the device and to enable/disable access to the device with different SNMP versions.

The SNMP agent enables access to the device management with SNMP-based applications.

**Configuration**

**SNMPv1**

Activates/deactivates the access to the device with SNMP version 1.

Possible values:
- **marked** (default setting)
  - Access is activated.
- **unmarked**
  - Access is deactivated.

You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.

**SNMPv2**

Activates/deactivates the access to the device with SNMP version 2.

Possible values:
- **marked** (default setting)
  - Access is activated.
- **unmarked**
  - Access is deactivated.

You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.

**SNMPv3**

Activates/deactivates the access to the device with SNMP version 3.

Possible values:
- **marked** (default setting)
  - Access is activated.
- **unmarked**
  - Access is deactivated.

Network management systems like Industrial HiVision use this protocol to communicate with the device.
UDP port

Specifies the number of the UDP port on which the SNMP agent receives requests from clients.

Possible values:
- 1..65535  (default setting: 161)
  
  Exception: Port 2222 is reserved for internal functions.

To enable the SNMP agent to use the new port after a change, you proceed as follows:

- Click the  button.
- Select in the Basic Settings > Load/Save dialog the active configuration profile.
- Click the  button to save the current settings.
- Restart the device.

SNMPover802

Activates/deactivates the access to the device through SNMP over IEEE-802.

Possible values:
- marked  Access is activated.
- unmarked  (default setting)  Access is deactivated.

[Telnet]

This tab lets you enable/disable the Telnet server in the device and specify its settings.

The Telnet server enables access to the device management remotely through the Command Line Interface. Telnet connections are unencrypted.

Operation

Telnet server

Enables/disables the Telnet server.

Possible values:
- On  (default setting)  The Telnet server is enabled.  The access to the device management is possible through the Command Line Interface using an unencrypted Telnet connection.
- Off  The Telnet server is disabled.

Note: If the SSH server is disabled and you also disable the Telnet server, then the access to the Command Line Interface is only possible through the serial interface of the device.
Device Security

[Device Security > Management Access > Server]

Configuration

TCP port

Specifies the number of the TCP port on which the device receives Telnet requests from clients.

Possible values:

- 1..65535  (default setting: 23)
  Exception: Port 2222 is reserved for internal functions.

The server restarts automatically after the port is changed. Existing connections remain in place.

Connections

Displays how many Telnet connections are currently established to the device.

Connections (max.)

Specifies the maximum number of Telnet connections to the device that can be set up simultaneously.

Possible values:

- 1..5  (default setting: 5)

Session timeout [min]

Specifies the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged in.

A change in the value takes effect the next time a user logs in.

Possible values:

- 0
  Deactivates the function. The connection remains established in the case of inactivity.
- 1..160  (default setting: 5)

[SSH]

This tab lets you enable/disable the SSH server in the device and specify its settings required for SSH. The server works with SSH version 2.

The SSH server enables access to the device management remotely through the Command Line Interface. SSH connections are encrypted.

The SSH server identifies itself to the clients using its public RSA key. When first setting up the connection, the client program displays the user the fingerprint of this key. The fingerprint contains a Base64-coded character sequence that is easy to check. When you make this character sequence available to the users through a reliable channel, they have the option to compare both fingerprints. If the character sequences match, then the client is connected to the correct server.
The device lets you create the private and public keys (host keys) required for RSA directly in the device. Otherwise you have the option to copy your own keys to the device in PEM format.

As an alternative, the device lets you load the RSA key (host key) from an external memory during the system startup. You activate this function in the Basic Settings > External Memory dialog, SSH key auto upload column.

**Operation**

**SSH server**

Enables/disables the SSH server.

Possible values:

- **On** (default setting)
  - The SSH server is enabled.
  - The access to the device management is possible through the Command Line Interface using an encrypted SSH connection.
  - You can start the server only if there is an RSA signature in the device.

- **Off**
  - The SSH server is disabled.
  - When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up.

**Note:** If the Telnet server is disabled and you also disable the SSH server, then the access to the Command Line Interface is only possible through the serial interface of the device.

**Configuration**

**TCP port**

Specifies the number of the TCP port on which the device receives SSH requests from clients.

Possible values:

- **1..65535** (default setting: 22)
  - Exception: Port 2222 is reserved for internal functions.

The server restarts automatically after the port is changed. Existing connections remain in place.

**Sessions**

Displays how many SSH connections are currently established to the device.
Sessions (max.)

Specifies the maximum number of SSH connections to the device that can be set up simultaneously.

Possible values:

- 1..5 (default setting: 5)

Session timeout [min]

Specifies the timeout in minutes. After the user logged in has been inactive for this time, the device ends the connection.

A change in the value takes effect the next time a user logs in.

Possible values:

- 0
  - Deactivates the function. The connection remains established in the case of inactivity.
- 1..160 (default setting: 5)

Signature

RSA present

Displays if an RSA host key is present in the device.

Possible values:

- marked
  - A key is present.
- unmarked
  - No key is present.

Create

Generates a host key in the device. The prerequisite is that the SSH server is disabled.

Length of the key created:

- 2048 bit (RSA)

To get the SSH server to use the generated host key, restart the SSH server.

Alternatively, you have the option to copy your own host key to the device in PEM format. See the Key import frame.

Delete

Removes the host key from the device. The prerequisite is that the SSH server is disabled.

Oper status

Displays if the device currently generates a host key.

It is possible that another user triggered this action.
Possible values:

- rsa
  The device currently generates an RSA host key.
- none
  The device does not generate a host key.

**Fingerprint**

The fingerprint is an easy to verify string that uniquely identifies the host key of the SSH server.

After importing a new host key, the device continues to display the existing fingerprint until you restart the server.

**Fingerprint type**

Specifies which fingerprint the *RSA fingerprint* field displays.

Possible values:

- md5
  The *RSA fingerprint* field displays the fingerprint as hexadecimal MD5 hash.
- sha256  (default setting)
  The *RSA fingerprint* field displays the fingerprint as Base64-coded SHA256 hash.

**RSA fingerprint**

Displays the fingerprint of the public host key of the SSH server.

When you change the settings in the *Fingerprint type* field, click afterwards the ✔ button and then the ⚪️ button to update the display.

**Key import**

**URL**

Specifies the path and file name of your own RSA host key.

The device accepts the RSA key if it has the following key length:
- 2048 bit (RSA)

The device gives you the following options for copying the key to the device:

- Import from the PC
  When the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the ⏳️ area. Alternatively click in the area to select the file.
- Import from an FTP server
  When the key is on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>:<port>/<file name>`
Import from a TFTP server
When the key is on a TFTP server, specify the URL for the file in the following form:
tftp://<IP address>/<path>/<file name>

Import from an SCP or SFTP server
When the key is on an SCP or SFTP server, specify the URL for the file in the following form:
scp://<IP address>/<path>/<file name>

When you click the Start button, the device displays the Credentials window. There you enter User name and Password, to log in to the server.
scp://<user>:<password>@<IP address>/<path>/<file name>

Start

Copies the key specified in the URL field to the device.

[HTTP]

This tab lets you enable/disable the HTTP protocol for the web server and specify the settings required for HTTP.

The web server provides the Graphical User Interface through an unencrypted HTTP connection. For security reasons, disable the HTTP protocol and use the HTTPS protocol instead.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

Note: If you change the settings in this tab and click the ✔ button, then the device ends the session and disconnects every opened connection. To continue working with the Graphical User Interface, log in again.

Operation

HTTP server

Enables/disables the HTTP protocol for the web server.

Possible values:

- **On** (default setting)
  - The HTTP protocol is enabled.
  - The access to the device management is possible through an unencrypted HTTP connection.
  - When the HTTPS protocol is also enabled, the device automatically redirects the request for a HTTP connection to an encrypted HTTPS connection.

- **Off**
  - The HTTP protocol is disabled.
  - When the HTTPS protocol is enabled, the access to the device management is possible through an encrypted HTTPS connection.

Note: If the HTTP and HTTPS protocols are disabled, then you can enable the HTTP protocol using the Command Line Interface command http server to get to the Graphical User Interface.
### Configuration

**TCP port**

Specifies the number of the TCP port on which the web server receives HTTP requests from clients.

Possible values:

- **1..65535** (default setting: 80)
  
  Exception: Port **2222** is reserved for internal functions.

### [HTTPS]

This tab lets you enable/disable the HTTPS protocol for the web server and specify the settings required for HTTPS.

The web server provides the Graphical User Interface through an encrypted HTTP connection.

A digital certificate is required for the encryption of the HTTP connection. The device lets you create this certificate yourself or to load an existing certificate onto the device.

The device supports up to 10 simultaneous connections using HTTP or HTTPS.

**Note:** If you change the settings in this tab and click the ✓ button, then the device ends the session and disconnects every opened connection. To continue working with the Graphical User Interface, log in again.

### Operation

**HTTPS server**

Enables/disables the HTTPS protocol for the web server.

Possible values:

- **On** (default setting)
  
  The HTTPS protocol is enabled.  
  The access to the device management is possible through an encrypted HTTPS connection. When there is no digital certificate present, the device generates a digital certificate before it enables the HTTPS protocol.

- **Off**
  
  The HTTPS protocol is disabled.  
  When the HTTP protocol is enabled, the access to the device management is possible through an unencrypted HTTP connection.

**Note:** If the HTTP and HTTPS protocols are disabled, then you can enable the HTTPS protocol using the Command Line Interface command `https server` to get to the Graphical User Interface.
Configuration

TCP port

Specifies the number of the TCP port on which the web server receives HTTPS requests from clients.

Possible values:
- 1..65535 (default setting: 443)
  
  Exception: Port 2222 is reserved for internal functions.

Certificate

If the device uses an HTTPS certificate not signed by a certification authority (CA) known to the web browser, then the web browser may display a warning message before loading the Graphical User Interface.

To address the warning, you have the following possibilities:
- Install an HTTPS certificate on the device whose CA is known to your web browser. This may additionally require you to make the CA known to your web browser or operating system.
- As a workaround, you can also add an exception rule for the existing device certificate in your web browser.

Present

Displays if the digital certificate is present in the device.

Possible values:
- marked
  The certificate is present.
- unmarked
  The certificate has been removed.

Create

Generates a digital certificate in the device.

Until restarting the web server uses the previous certificate.

To get the web server to use the newly generated certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

Alternatively, you have the option of copying your own certificate to the device. See the Certificate import frame.

Delete

Deletes the digital certificate.

Until restarting the web server uses the previous certificate.
Oper status

Displays if the device currently generates or deletes a digital certificate.

It is possible that another user has triggered the action.

Possible values:

- none
  The device does currently not generate or delete a certificate.
- delete
  The device currently deletes a certificate.
- generate
  The device currently generates a certificate.

Fingerprint

The fingerprint is an easily verified hexadecimal number sequence that uniquely identifies the digital certificate of the HTTPS server.

After importing a new digital certificate, the device displays the current fingerprint until you restart the server.

Fingerprint type

Specifies which fingerprint the Fingerprint field displays.

Possible values:

- sha1
  The Fingerprint field displays the SHA1 fingerprint of the certificate.
- sha256 (default setting)
  The Fingerprint field displays the SHA256 fingerprint of the certificate.

Fingerprint

Hexadecimal character sequence of the digital certificate used by the server.

When you change the settings in the Fingerprint type field, click afterwards the button and then the button to update the display.

Certificate import

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
• **Base64-coded, enclosed by**
  
  ```
  -----BEGIN PRIVATE KEY-----
  and
  -----END PRIVATE KEY-----
  and
  -----BEGIN CERTIFICATE-----
  and
  -----END CERTIFICATE-----
  ```

• **RSA key with 2048 bit length**

The device gives you the following options for copying the certificate to the device:

- **Import from the PC**
  When the certificate is located on your PC or on a network drive, drag and drop the certificate onto the **area. Alternatively click in the area to select the certificate.**

- **Import from an FTP server**
  When the certificate is on an FTP server, specify the URL for the file in the following form:
  
  `ftp://<user>:<password>@<IP address>[:port]/<path>/<file name>`

- **Import from a TFTP server**
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  
  `tftp://<IP address>/<path>/<file name>`

- **Import from an SCP or SFTP server**
  When the certificate is on an SCP or SFTP server, specify the URL for the file in the following form:
  
  `- scp://<IP address>[:port]/<path>/<file name>  
  `- sftp://<user>:<password>@<IP address>[:port]/<path>/<file name>  

When you click the **Start** button, the device displays the **Credentials** window. There you enter **User name** and **Password**, to log in to the server.

Options:

- scp:// or sftp://<IP address>[:port]/<path>/<file name>

Start

Copies the certificate specified in the **URL** field to the device.
### 3.4.2 IP Access Restriction

This dialog lets you restrict the access to the device management to specific IP address ranges and selected IP-based applications.

- If the function is disabled, then the access to the device management is possible from any IP address and using every application.
- If the function is enabled, then the access is restricted. You have access to the device management only under the following conditions:
  - At least one table row is activated.
  - You are accessing the device with a permitted application from a permitted IP address range.

**Operation**

**Note:** Before you enable the function, verify that at least one active table row in the table lets you access. Otherwise, if you change the settings, then the connection to the device terminates. The access to the device management is possible only using the Command Line Interface through the serial interface.

#### Operation

Enables/disables the *IP Access Restriction* function.

Possible values:

- **On**  
  The *IP Access Restriction* function is enabled.  
  The access to the device management is restricted.

- **Off** (default setting)  
  The *IP Access Restriction* function is disabled.

#### Table

You have the option of defining up to 16 table rows and activating them separately.

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

#### Buttons

- ![Add](image)  
  Adds a table row.

- ![Remove](image)  
  Removes the selected table row.
### Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

When you delete a table row, this leaves a gap in the numbering. When you create a new table row, the device fills the first gap.

Possible values:

- **1..16**

### Address

Specifies the IP address of the network from which you allow the access to the device management. You specify the network range in the *Netmask* column.

Possible values:

- **Valid IPv4 address** (default setting: **0.0.0.0**)

### Netmask

Specifies the range of the network specified in the *Address* column.

Possible values:

- **Valid netmask** (default setting: **0.0.0.0**)

### HTTP

Activates/deactivates the HTTP access.

Possible values:

- **marked** (default setting)
  - Access is activated for the adjacent IP address range.
- **unmarked**
  - Access is deactivated.

### HTTPS

Activates/deactivates the HTTPS access.

Possible values:

- **marked** (default setting)
  - Access is activated for the adjacent IP address range.
- **unmarked**
  - Access is deactivated.

### SNMP

Activates/deactivates the SNMP access.

Possible values:

- **marked** (default setting)
  - Access is activated for the adjacent IP address range.
- **unmarked**
  - Access is deactivated.
Telnet

Activates/deactivates the Telnet access.

Possible values:
- **marked** (default setting)
  Access is activated for the adjacent IP address range.
- **unmarked**
  Access is deactivated.

SSH

Activates/deactivates the SSH access.

Possible values:
- **marked** (default setting)
  Access is activated for the adjacent IP address range.
- **unmarked**
  Access is deactivated.

IEC61850-MMS

Activates/deactivates the access to the MMS server.

Possible values:
- **marked** (default setting)
  Access is activated for the adjacent IP address range.
- **unmarked**
  Access is deactivated.

Modbus TCP

Activates/deactivates the access to the **Modbus TCP** server.

Possible values:
- **marked** (default setting)
  Access is activated for the adjacent IP address range.
- **unmarked**
  Access is deactivated.

Active

Activates/deactivates the table row.

Possible values:
- **marked** (default setting)
  The table row is activated. The device restricts the access to the device management to the adjacent IP address range and the selected IP-based applications.
- **unmarked**
  The table row is deactivated.
3.4.3 Web

In this dialog you specify settings for the Graphical User Interface.

Configuration

Web interface session timeout [min]

Specifies the timeout in minutes. After the device has been inactive for this time it ends the session for the user logged in.

Possible values:

- 0..160 (default setting: 5)

The value 0 deactivates the function, and the user remains logged in when inactive.
3.4.4 Command Line Interface

In this dialog you specify settings for the Command Line Interface. For further information about the Command Line Interface, see the “Command Line Interface” reference manual.

The dialog contains the following tabs:
- [Global]
- [Login banner]

[Global]

This tab lets you change the prompt in the Command Line Interface and specify the automatic closing of sessions through the serial interface when they have been inactive.

The device has the following serial interfaces.
- USB-C interface

Configuration

Login prompt

Specifies the character string that the device displays in the Command Line Interface at the start of every command line.

Possible values:
- Alphanumeric ASCII character string with 0..128 characters (0x20..0x7E) including space characters
- Wildcards
  - %d date
  - %i IP address
  - %m MAC address
  - %p product name
  - %t time
- Default setting: (GRS)

Changes to this setting are immediately effective in the active Command Line Interface session.

Serial interface timeout [min]

Specifies the time in minutes after which the device automatically closes the session of an inactive user logged in with the Command Line Interface through the serial interface.

Possible values:
- 0..160 (default setting: 5)
  - The value 0 deactivates the function, and the user remains logged in when inactive.

A change in the value takes effect the next time a user logs in.

For the Telnet server and the SSH server, you specify the timeout in the Device Security > Management Access > Server dialog.
[Login banner]

In this tab you replace the start screen of the Command Line Interface with your own text.

In the default setting, the start screen displays information about the device, such as the software version and the device settings. With the function in this tab, you deactivate this information and replace it with an individually specified text.

To display your own text in the Command Line Interface and in the Graphical User Interface before the login, you use the Device Security > Pre-login Banner dialog.

**Operation**

Operation

Enables/disables the Login banner function.

Possible values:

- **On**
  The Login banner function is enabled. The device displays the text information specified in the Banner text field to the users that log in with the Command Line Interface.

- **Off** (default setting)
  The Login banner function is disabled. The start screen displays information about the device. The text information in the Banner text field is kept.

**Banner text**

Banner text

Specifies the character string that the device displays in the Command Line Interface at the start of every session.

Possible values:

- Alphanumeric ASCII character string with 0..1024 characters (0x20..0x7E) including space characters
- `<Tab>`
- `<Line break>`
3.4.5 **SNMPv1/v2 Community**

In this dialog you specify the community name for SNMPv1/v2 applications.

Applications send requests using SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name, the application gets read authorization or read and write authorization for the device.

You activate the access to the device using SNMPv1/v2 in the *Device Security > Management Access > Server* dialog.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Community</th>
<th>Displays the authorization for SNMPv1/v2 applications to the device:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write</td>
<td>For requests with the community name entered, the application receives read and write authorization for the device.</td>
</tr>
<tr>
<td>Read</td>
<td>For requests with the community name entered, the application receives read authorization for the device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies the community name for the adjacent authorization.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>Alphanumeric ASCII character string with 0..32 characters</td>
<td></td>
</tr>
<tr>
<td>private</td>
<td>(default setting for read and write authorizations)</td>
</tr>
<tr>
<td>public</td>
<td>(default setting for read authorization)</td>
</tr>
</tbody>
</table>
3.5 Pre-login Banner

This dialog lets you display a greeting or information text to users before they log in.

The users see this text in the login dialog of the Graphical User Interface and of the Command Line Interface. Users logging in with SSH see the text - regardless of the client used - before or during the login.

To display the text only in the Command Line Interface, use the settings in the Device Security > Management Access > CLI dialog.

Operation

Enables/disables the Pre-login Banner function.

Using the Pre-login Banner function, the device displays a greeting or information text in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

- **On**
  - The Pre-login Banner function is enabled. The device displays the text specified in the Banner text field in the login dialog.
  - **Off** (default setting)
  - The Pre-login Banner function is disabled. The device does not display a text in the login dialog. When you enter a text in the Banner text field, this text is saved in the device.

Banner text

Specifies information text that the device displays in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

- Alphanumeric ASCII character string with 0..512 characters (0x20..0x7E) including space characters
- `<Tab>`
- `<Line break>`
4 Network Security

The menu contains the following dialogs:

- Network Security Overview
- Port Security
- 802.1X
- RADIUS
- DoS
- ACL

4.1 Network Security Overview

This dialog displays an overview over the network security rules used in the device.

Overview

The top level displays:

- The ports to which a network security rule is assigned.
- The VLANs to which a network security rule is assigned.

The subordinate levels display:

- The ACL rules specified. See the Network Security > ACL dialog.

Buttons

Displays a text field to search for a keyword. When you enter a character or string, the overview displays only items related to this keyword.

Collapses the levels. The overview then displays only the first level of the items.

Expands the levels. The overview then displays every level of the items.

Expands the current item and displays the items of the next lower level.

Collapses the item and hides the items of the underlying levels.
4.2 Port Security

The device lets you forward only data packets from desired senders on a port. When the Port Security function is enabled, the device checks the VLAN ID and MAC address of the sender before it forwards a data packet. The device discards data packets from not desired senders and logs this event.

In this dialog, a Wizard window helps you associate the ports with the address of one or more desired senders. In the device, these addresses are known as static entries. To view the specified static addresses, select the relevant port and click the button.

To simplify the setup process, the device lets you record the address of the desired senders automatically. The device “learns” the addresses by evaluating the received data packets. In the device, these addresses are known as dynamic entries. When a user-defined upper limit has been reached (Dynamic limit), the device stops the “learning” on the relevant port. The device forwards only the data packets of the senders already registered on the port. When you adapt the upper limit to the number of expected senders, you thus make MAC Flooding attacks more difficult.

Note: With the automatic recording of the dynamic entries, the device constantly discards the first data packet from unknown senders. Using this first data packet, the device checks if the upper limit has been reached. The device records the addresses until the upper limit is reached. Afterwards, the device forwards data packets that it receives on the relevant port from this sender.

Operation

Enables/disables the Port Security function in the device.

Possible values:

- **On**: The Port Security function is enabled. The device checks the VLAN ID and the source MAC address before it forwards a data packet. The device forwards a received data packet only if the VLAN ID and the source MAC address of the data packet are desired on the relevant port. For this setting to take effect, you also activate the Port Security function on the relevant ports.

- **Off** (default setting): The Port Security function is disabled. The device forwards every received data packet without checking the source address.
Network Security

[Network Security > Port Security]

Configuration

Auto-disable

Activates/deactivates the Auto-Disable function for Port Security in the device.

Possible values:

- marked
  The Auto-Disable function for Port Security is active.
  Also mark the checkbox in the Auto-disable column for the relevant ports.
  The device disables the port and optionally sends an SNMP trap when one of the following events occurs:
  - The device registers at least one address of a sender that is not desired on the port.
  - The device registers more addresses than specified in the Dynamic limit column.

- unmarked (default setting)
  The Auto-Disable function for Port Security is inactive.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Wizard

Opens the Wizard window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: Port security]” on page 127.

Port

Displays the port number.

Active

Activates/deactivates the Port Security function on the port.

Possible values:

- marked
  The device checks every data packet received on the port and forwards it only if the source address of the data packet is desired. Also enable the Port Security function in the Operation frame.

- unmarked (default setting)
  The device forwards every data packet received on the port without checking the source address.

Note: When you operate the device as an active participant within an MRP ring, we recommend that you unmark the checkbox for the ring ports.
Auto-disable

Activates/deactivates the Auto-Disable function for Port Security on the port.

Possible values:

- **marked** (default setting)
  - The Auto-Disable function is active on the port.
  - The device disables the port and optionally sends an SNMP trap when one of the following events occurs:
    - The device registers at least one address of a sender that is not desired on the port.
    - The device registers more addresses than specified in the Dynamic limit column.
  - The Link status LED for the port flashes 3× per period. This restriction makes MAC Spoofing attacks more difficult.
  - The prerequisite is that in the Configuration frame the Auto-disable checkbox is marked.
  - The Diagnostics > Ports > Auto-Disable dialog displays which ports are currently disabled due to the parameters being exceeded.
  - After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the Diagnostics > Ports > Auto-Disable dialog and specify a waiting period for the relevant port in the Reset timer [s] column.

- **unmarked**
  - The Auto-Disable function is inactive on the port.

Send trap

Activates/deactivates the sending of SNMP traps when the device discards a data packet from an undesired sender on the port.

Possible values:

- **marked**
  - The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
  - If the device discards data packets from a sender that is not desired on the port, then the device sends an SNMP trap.

- **unmarked** (default setting)
  - The sending of SNMP traps is inactive.

Trap interval [s]

Specifies the delay time in seconds that the device waits after sending an SNMP trap before sending the next SNMP trap.

Possible values:

- **0..3600** (default setting: 0)
  - The value 0 deactivates the delay time.

Dynamic limit

Specifies the upper limit for the number of automatically registered addresses (dynamic entries). When the upper limit is reached, the device stops “learning” on this port.

Adjust the value to the number of expected senders.

If the port registers more addresses than specified here, then the Auto-Disable function disables the port. The prerequisite is that you mark the checkbox in the Auto-disable column and the Auto-disable checkbox in the Configuration frame.
Possible values:

- **0**: No automatic registering of addresses on this port.
- **1..600** (default setting: **600**)

### Static limit

Specifies the upper limit for the number of addresses associated with the port using the *Wizard* window (**static entries**).

Possible values:

- **0**: No association possible between the port and a desired sender. Only specify this value if you specify a value > 0 in the *Dynamic limit* column.
- **1..64** (default setting: **64**)

### Dynamic entries

Displays the number of addresses that the device has automatically registered.

### Static MAC entries

Displays the number of MAC addresses associated with the port.

### Last violating VLAN ID/MAC

Displays the VLAN ID and MAC address of an undesired sender whose data packets the device last discarded on this port.

### Sent traps

Displays the number of discarded data packets on this port that caused the device to send an SNMP trap.

### [Wizard: Port security]

The *Wizard* window helps you associate the ports with the address of one or more desired senders.

The *Wizard* window guides you through the following steps:

- **Select port**
- **MAC addresses**

**Note:** The device saves the addresses associated with the port until you deactivate the *Port Security* function on the relevant port or disable the *Port Security* function in the device.

After closing the *Wizard* window, click the ✓ button to save your settings.
Select port

Port

Specifies the port that you associate with the address of desired senders in the next step.

MAC addresses

Static entries (x/y)

Displays the number of addresses associated with the port using the Wizard window and the upper limit for static entries. The lower part of the Wizard window displays the entries in detail, if any.

Removes the entries in the lower part of the Wizard window. The device removes the respective association between a port and the desired senders.

VLAN ID

Specifies the VLAN ID of the desired sender.

Possible values:

1..4042

MAC address

Specifies the MAC address of the desired sender.

Possible values:

- Valid Unicast MAC address
  Specify the value with a colon separator, for example 00:11:22:33:44:55.

Note: You can assign a MAC address to only one port.

Add

Creates a static entry based on the values specified in the VLAN ID and MAC address fields. As a result, you find a new entry in the lower part of the Wizard window.
Entries in the lower part of the window

The lower part of the *Wizard* window displays the VLAN ID and MAC address of desired senders on this port. In the following list you find a description of the icons specific to these entries.

- **Static entry**: When you click the icon, the device removes the *static entry* and the respective association between the port and the desired senders.

- **Dynamic entry**: When you click the icon, the icon changes to ⭐. The device converts the *dynamic entry* to a *static entry* when you close the *Wizard* window. To undo this change, click the icon again before you close the *Wizard* window.

### 4.3 802.1X

With the port-based access control according to IEEE 802.1X, the device monitors the access to the network from connected end devices. The device (authenticator) lets an end device (supplicant) have access to the network if it logs in with valid login data. The authenticator and the end devices communicate using the EAPoL (Extensible Authentication Protocol over LANs) authentication protocol.

The device supports the following methods to authenticate end devices:

- **radius**
  - A RADIUS server in the network authenticates the end devices.

- **ias**
  - The Integrated Authentication Server (IAS) implemented in the device authenticates the end devices. Compared to RADIUS, the IAS provides only basic functions.

The menu contains the following dialogs:

- 802.1X Global
- 802.1X Port Configuration
- 802.1X Port Clients
- 802.1X EAPOL Port Statistics
- 802.1X Port Authentication History
- 802.1X Integrated Authentication Server
4.3.1 802.1X Global

This dialog lets you specify basic settings for the port-based access control.

**Operation**

Enables/disables the 802.1X function.

Possible values:

- **On**
  
  The 802.1X function is enabled.
  
  The device checks the access to the network from connected end devices.
  
  The port-based access control is enabled.

- **Off** (default setting)
  
  The 802.1X function is disabled.
  
  The port-based access control is disabled.

**Configuration**

**VLAN assignment**

Activates/deactivates the assigning of the relevant port to a VLAN. This function lets you provide selected services to the connected end device in this VLAN.

Possible values:

- **marked**
  
  The assigning is active.
  
  If the end device successfully authenticates itself, then the device assigns to the relevant port the VLAN ID transferred by the RADIUS authentication server.

- **unmarked** (default setting)
  
  The assigning is inactive.
  
  The relevant port is assigned to the VLAN specified in the Network Security > 802.1X > Port Configuration dialog, Assigned VLAN ID column.

**Dynamic VLAN creation**

Activates/deactivates the automatic creation of the VLAN assigned by the RADIUS authentication server if the VLAN does not exist.

Possible values:

- **marked**
  
  The automatic VLAN creation is active.
  
  The device creates the VLAN if it does not exist.

- **unmarked** (default setting)
  
  The automatic VLAN creation is inactive.
  
  If the assigned VLAN does not exist, then the port remains assigned to the original VLAN.
Monitor mode

Activates/deactivates the monitor mode.

Possible values:

- **marked**
  The monitor mode is active. The device monitors the authentication and helps with diagnosing detected errors. If an end device has not logged in successfully, then the device gives the end device access to the network.

- **unmarked** (default setting)
  The monitor mode is inactive.

**Information**

Monitor mode clients

Displays how many end devices the device gave network access even though they did not log in successfully.

The prerequisite is that in the Configuration frame the Monitor mode function is active.

Non monitor mode clients

Displays the number of end devices to which the device gave network access after successful login.

Policy 1

Displays the method that the device currently uses to authenticate the end devices using IEEE 802.1X.

You specify the method used in the Device Security > Authentication List dialog.

- To authenticate the end devices through a RADIUS server, you assign the *radius* policy to the 8021x list.
- To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the *ias* policy to the 8021x list.
4.3.2 802.1X Port Configuration

This dialog lets you specify the access settings for every port.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Port**

Displays the port number.

**Port initialization**

Activates/deactivates the port initialization in order to activate the access control on the port or reset it to its initial state. Use this function only on ports in which the Port control column contains the value auto.

Possible values:

- **marked**
  The port initialization is active.
  When the initialization is complete, the device changes the value to **unmarked** again.

- **unmarked** (default setting)
  The port initialization is inactive.
  The device keeps the current port status.

**Port reauthentication**

Activates/deactivates the one-time reauthentication request.

Use this function only on ports in which the Port control column contains the value auto.

The device also lets you periodically request the end device to log in again. See the Periodic reauthentication column.

Possible values:

- **marked**
  The one-time reauthentication request is active.
  The device requests the end device to log in again. Afterwards, the device changes the value to unmarked again.

- **unmarked** (default setting)
  The one-time reauthentication request is inactive.
  The device keeps the end device logged in.

**Authentication activity**

Displays the current status of the Authenticator (Authenticator PAE state).

Possible values:

- **initialize**
- **disconnected**
Backend authentication state

Displays the current status of the connection to the authentication server (Backend Authentication state).

Possible values:
- request
- response
- success
- fail
- timeout
- idle
- initialize

Authentication state

Displays the current status of the authentication on the port (Controlled Port Status).

Possible values:
- authorized
  The end device is logged in successfully.
- unauthorized
  The end device is not logged in.

Port control

Specifies how the device grants access to the network (Port control mode).

Possible values:
- forceUnauthorized
  The device blocks the access to the network. You use this setting if an end device is connected to the port that does not receive access to the network.
- auto
  The device grants access to the network if the end device logged in successfully. You use this setting if an end device is connected to the port that logs in at the authenticator.

Note: If other end devices are connected through the same port, then they get access to the network without additional authentication.

- forceAuthorized (default setting)
  When end devices do not support IEEE 802.1X, the device grants access to the network. You use this setting if an end device is connected to the port that receives access to the network without logging in.
Quiet period [s]

Specifies the time period in seconds in which the authenticator does not accept any more logins from the end device after an unsuccessful login attempt (Quiet period [s]).

Possible values:
- 0..65535 (default setting: 60)

Transmit period [s]

Specifies the period in seconds after which the authenticator requests the end device to log in again. After this waiting period, the device sends an EAP request/identity data packet to the end device.

Possible values:
- 1..65535 (default setting: 30)

Supplicant timeout period [s]

Specifies the period in seconds for which the authenticator waits for the login of the end device.

Possible values:
- 1..65535 (default setting: 30)

Server timeout [s]

Specifies the period in seconds for which the authenticator waits for the response from the authentication server (RADIUS or IAS).

Possible values:
- 1..65535 (default setting: 30)

Requests (max.)

Specifies how many times the authenticator requests the end device to log in until the time specified in the Supplicant timeout period [s] column has elapsed. The device sends an EAP request/identity data packet to the end device as often as specified here.

Possible values:
- 0..10 (default setting: 2)

Assigned VLAN ID

Displays the ID of the VLAN that the authenticator assigned to the port. This value applies only on ports in which the Port control column contains the value auto.

Possible values:
- 0..4042 (default setting: 0)

You find the VLAN ID that the authenticator assigned to the ports in the Network Security > 802.1X > Port Clients dialog.
Assignment reason
Displays the cause for the assignment of the VLAN ID. This value applies only on ports in which the *Port control* column contains the value *auto*.

Possible values:
- *notAssigned* (default setting)
- *radius*
- *guestVlan*
- *unauthenticatedVlan*

You find the VLAN ID that the authenticator assigned to the ports for a supplicant in the *Network Security > 802.1X > Port Clients* dialog.

Reauthentication period [s]
Specifies the period in seconds after which the authenticator periodically requests the end device to log in again.

Possible values:
- *1..65535* (default setting: *3600*)

Periodic reauthentication
Activates/deactivates periodic reauthentication requests.

Possible values:
- *marked*
The periodic reauthentication requests are active.
The device periodically requests the end device to log in again. You specify this time period in the *Reauthentication period [s]* column.
If the authenticator assigned the ID of a Voice VLAN, Unauthenticated VLAN or Guest VLAN to the end device, then this setting becomes ineffective.
- *unmarked* (default setting)
The periodic reauthentication requests are inactive.
The device keeps the end device logged in.

Guest VLAN ID
Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in during the time period specified in the *Guest VLAN period* column. This value applies only on ports in which the *Port control* column contains the value *auto*.

This function lets you grant end devices, without IEEE 802.1X support, access to selected services in the network.

Possible values:
- *0* (default setting)
The authenticator does not assign a Guest VLAN to the port.
- *1..4042*

*Note:* The *MAC authorized bypass* function and the *Guest VLAN ID* function cannot be in use simultaneously.
Guest VLAN period

Displays the period in seconds for which the authenticator waits for EAPOL data packets after the end device is connected. If this period elapses, then the authenticator grants the end device access to the network and assigns the port to the Guest VLAN specified in the Guest VLAN ID column.

The value in this column is the triple of the value specified in the Transmit period [s] column.

Unauthenticated VLAN ID

Specifies the ID of the VLAN that the authenticator assigns to the port if the end device does not log in successfully. This value applies only on ports in which the Port control column contains the value auto.

This function lets you grant end devices without valid login data access to selected services in the network.

Possible values:

- 0..4042 (default setting: 0)

The effect of the value 0 is that the authenticator does not assign a Unauthenticated VLAN to the port.

Note: Assign to the port a VLAN set up statically in the device.
4.3.3 802.1X Port Clients

This dialog displays information on the connected end devices.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

| Port | Displays the port number. |
| User name | Displays the user name with which the end device logged in. |
| MAC address | Displays the MAC address of the end device. |
| Assigned VLAN ID | Displays the VLAN ID that the authenticator assigned to the port after the successful authentication of the end device. |
| Assignment reason | Displays the reason for the assignment of the VLAN. Possible values: default, radius, unauthenticatedVlan, guestVlan, monitorVlan, invalid. The field only displays a valid value as long as the client is authenticated. |
| Session timeout | Displays the remaining time in seconds until the login of the end device expires. This value applies only if for the port in the Network Security > 802.1X > Port Configuration dialog, Port control column the value auto is specified. The authentication server assigns the timeout period to the device through RADIUS. The value 0 means that the authentication server has not assigned a timeout. |
Termination action

Displays the action performed by the device when the login has elapsed.

Possible values:

- default
- reauthenticate
4.3.4 802.1X EAPOL Port Statistics

This dialog displays which EAPOL data packets the end device has sent and received for the authentication of the end devices.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Remove**
  
  Removes the selected table row.

**Port**

Displays the port number.

**Received packets**

Displays the total number of EAPOL data packets that the device received on the port.

**Transmitted packets**

Displays the total number of EAPOL data packets that the device sent on the port.

**Start packets**

Displays the number of EAPOL start data packets that the device received on the port.

**Logoff packets**

Displays the number of EAPOL logoff data packets that the device received on the port.

**Response/ID packets**

Displays the number of EAP response/identity data packets that the device received on the port.

**Response packets**

Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).

**Request/ID packets**

Displays the number of EAP request/identity data packets that the device received on the port.
Request packets

Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).

Invalid packets

Displays the number of EAPOL data packets with an unknown frame type that the device received on the port.

Received error packets

Displays the number of EAPOL data packets with an invalid packet body length field that the device received on the port.

Packet version

Displays the protocol version number of the EAPOL data packet that the device last received on the port.

Source of last received packet

Displays the sender MAC address of the EAPOL data packet that the device last received on the port.

The value 00:00:00:00:00:00 means that the port has not received any EAPOL data packets yet.
4.3.5 **802.1X Port Authentication History**

The device registers the authentication process of the end devices that are connected to its ports. This dialog displays the information recorded during the authentication.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- ![Remove](image) **Remove**
  
  Removes the selected table row.

**Port**

Displays the port number.

**Authentication time stamp**

Displays the time at which the authenticator authenticated the end device.

**Result age**

Displays since when this entry has been entered in the table.

**MAC address**

Displays the MAC address of the end device.

**VLAN ID**

Displays the ID of the VLAN that was assigned to the end device before the login.

**Authentication status**

Displays the status of the authentication on the port.

Possible values:

- **success**
  
  The authentication was successful.

- **failure**
  
  The authentication did not succeed.
Network Security

Access status
Displays if the device grants the end device access to the network.

Possible values:
- granted
  The device grants the end device access to the network.
- denied
  The device denies the end device access to the network.

Assigned VLAN ID
Displays the ID of the VLAN that the authenticator assigned to the port.

Assignment type
Displays the type of the VLAN that the authenticator assigned to the port.

Possible values:
- default
- radius
- unauthenticatedVlan
- guestVlan
- monitorVlan
- notAssigned

Assignment reason
Displays the reason for the assignment of the VLAN ID and the VLAN type.
### 4.3.6 802.1X Integrated Authentication Server

The Integrated Authentication Server (IAS) lets you authenticate end devices using IEEE 802.1X. Compared to RADIUS, the IAS has a very limited range of functions. The authentication is based only on the user name and the password.

In this dialog you manage the login data of the end devices. The device lets you set up to 100 sets of login data.

To authenticate the end devices through the Integrated Authentication Server you assign in the Device Security > Authentication List dialog the `ias` policy to the 8021x list.

**Table**

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

**Buttons**

- **Add**
  
  Opens the **Create** window to add a table row.
  
  ▶ In the **User name** field, you specify the name of the user account on the end device.

- **Remove**
  
  Removes the selected table row.

**User name**

Displays the name of the user account on the end device.

To create a new user, click the **Add** button.

**Password**

Specifies the password with which the user authenticates.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters

The device differentiates between upper and lower case.
Active

Activates/deactivates the login data.

Possible values:

- **marked**
  The login data is active. An end device has the option of logging in through IEEE 802.1X using this login data.

- **unmarked** (default setting)
  The login data is inactive.

### 4.4 RADIUS

With its factory settings, the device authenticates users based on the local user management. However, as the size of a network increases, it becomes more difficult to keep the login data of the users consistent across the devices.

RADIUS (Remote Authentication Dial-In User Service) lets you authenticate and authorize the users at a central point in the network. A RADIUS server performs the following tasks here:

- **Authentication**
  The authentication server authenticates the users when the RADIUS client at the access point forwards the login data of the users to the server.

- **Authorization**
  The authentication server authorizes logged in users for selected services by assigning various parameters for the relevant end device to the RADIUS client at the access point.

- **Accounting**
  The accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. This lets you subsequently determine which services the users have used, and to what extent.

If you assign the `radius` policy to an application in the **Device Security > Authentication List** dialog, then the device operates in the role of the RADIUS client. The device forwards the login data of the users to the primary authentication server. The authentication server decides if the login data is valid and transfers the authorizations of the users to the device.

The device assigns the Service Type transferred in the response of a RADIUS server as follows to an access role existing in the device:

- **Administrative-User**: administrator
- **Login-User**: operator
- **NAS-Prompt-User**: guest

The device also lets you authenticate end devices with IEEE 802.1X through an authentication server. To do this, you assign the `radius` policy to the `8021x` list in the **Device Security > Authentication List** dialog.

The menu contains the following dialogs:

- **RADIUS Global**
- **RADIUS Authentication Server**
- **RADIUS Accounting Server**
- **RADIUS Authentication Statistics**
- **RADIUS Accounting Statistics**
4.4.1 **RADIUS Global**

This dialog lets you specify basic settings for RADIUS.

**RADIUS configuration**

**Buttons**

- **Reset**


**Retransmits (max.)**

Specifies how many times the device retransmits an unanswered request to the authentication server before the device sends the request to an alternative authentication server.

Possible values:

- 1..15 (default setting: 4)

**Timeout [s]**

Specifies how many seconds the device waits for a response after a request to an authentication server before it retransmits the request.

Possible values:

- 1..30 (default setting: 5)

**Accounting**

Activates/deactivates the accounting.

Possible values:

- **marked**
  
  Accounting is active.
  
  The device sends the traffic data to an accounting server specified in the Network Security > RADIUS > Accounting Server dialog.

- **unmarked** (default setting)
  
  Accounting is inactive.

**NAS IP address (attribute 4)**

Specifies the IP address that the device transfers to the authentication server as attribute 4. Specify the IP address of the device or another available address.

**Note:** The device only includes the attribute 4 if the packet was triggered by the 802.1X authentication request of an end device (supplicant).
Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)

In many cases, there is a firewall between the device and the authentication server. In the Network Address Translation (NAT) in the firewall changes the original IP address, and the authentication server receives the translated IP address of the device.

The device transfers the IP address in this field unchanged across the Network Address Translation (NAT).
4.4.2 RADIUS Authentication Server

This dialog lets you specify up to 8 authentication servers. An authentication server authenticates and authorizes the users when the device forwards the login data to the server.

The device sends the login data to the specified primary authentication server. When the server does not respond, the device contacts the specified authentication server that is highest in the table. When no response comes from this server either, the device contacts the next server in the table.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the Create window to add a table row.

- In the Index field, you specify the index number.
- In the Address field, you specify the IP address of the server.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. You specify the index number when you add a table row.

Name

Displays the name of the server. To change the value, click the relevant field.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters (default setting: Default-RADIUS-Server)
  - You can specify the same name for several servers. When several servers have the same name, the setting in the Primary server column applies.
Network Security

(Network Security > RADIUS > Authentication Server)

Address

Specifies the IP address of the server.

Possible values:

- Valid IPv4 address

Destination UDP port

Specifies the number of the UDP port on which the server receives requests.

Possible values:

- **0..65535** (default setting: **1812**)
  
  Exception: Port **2222** is reserved for internal functions.

Secret

Displays ***** (asterisks) when you specify a password with which the device logs in to the server. To change the password, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 1..64 characters

You get the password from the administrator of the authentication server.

Primary server

Specifies the authentication server as primary or secondary.

Possible values:

- **marked**
  
  The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server. This setting applies only if more than one server in the table has the same value in the **Name** column.

- **unmarked** (default setting)
  
  The server is the secondary authentication server. When the device does not receive a response from the primary authentication server, the device sends the login data to the secondary authentication server.

Active

Activates/deactivates the connection to the server.

The device uses the server, if you specify in the **Device Security > Authentication List** dialog the value **radius** in one of the columns **Policy 1** to **Policy 5**.

Possible values:

- **marked** (default setting)
  
  The connection is active. The device sends the login data for authenticating the users to this server if the preconditions named above are fulfilled.

- **unmarked**
  
  The connection is inactive. The device does not send any login data to this server.
4.4.3 RADIUS Accounting Server

This dialog lets you specify up to 8 accounting servers. An accounting server records the traffic data that has occurred during the port authentication according to IEEE 802.1X. The prerequisite is that in the Network Security > RADIUS > Global dialog the Accounting function is active.

The device sends the traffic data to the first accounting server that can be reached. When the accounting server does not respond, the device contacts the next server in the table.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add
Opens the Create window to add a table row.
- In the Index field, you specify the index number.
- In the Address field, you specify the IP address of the server.

Remove
Removes the selected table row.

Index

Displays the index number to which the table row relates. You specify the index number when you add a table row.

Possible values:
- 1..8

Name

Displays the name of the server.

To change the value, click the relevant field.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters (default setting: Default-RADIUS-Server)
Address

Specifies the IP address of the server.

Possible values:
- Valid IPv4 address

Destination UDP port

Specifies the number of the UDP port on which the server receives requests.

Possible values:
- 0..65535 (default setting: 1813)
  Exception: Port 2222 is reserved for internal functions.

Secret

Displays ***** (asterisks) when you specify a password with which the device logs in to the server. To change the password, click the relevant field.

Possible values:
- Alphanumeric ASCII character string with 1..16 characters

You get the password from the administrator of the authentication server.

Active

Activates/deactivates the connection to the server.

Possible values:
- marked (default setting)
  The connection is active. The device sends traffic data to this server if the preconditions named above are fulfilled.
- unmarked
  The connection is inactive. The device does not send any traffic data to this server.
4.4.4 **RADIUS Authentication Statistics**

This dialog displays information about the communication between the device and the authentication server. The table displays the information for each server in a separate table row.

To delete the statistic, click in the *Network Security > RADIUS > Global* dialog the button.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

- **Name**
  - Displays the name of the server.

- **Address**
  - Displays the IP address of the server.

- **Round trip time**
  - Displays the time interval in hundredths of a second between the last response received from the server (Access Reply/Access Challenge) and the corresponding data packet sent (Access Request).

- **Access requests**
  - Displays the number of access data packets that the device sent to the server. This value does not take repetitions into account.

- **Retransmitted access-request packets**
  - Displays the number of access data packets that the device retransmitted to the server.

- **Access accepts**
  - Displays the number of access accept data packets that the device received from the server.

- **Access rejects**
  - Displays the number of access reject data packets that the device received from the server.

- **Access challenges**
  - Displays the number of access challenge data packets that the device received from the server.

- **Malformed access responses**
  - Displays the number of malformed access response data packets that the device received from the server (including data packets with an invalid length).
Bad authenticators

Displays the number of access response data packets with an invalid authenticator that the device received from the server.

Pending requests

Displays the number of access request data packets that the device sent to the server to which it has not yet received a response from the server.

Timeouts

Displays how many times no response to the server was received before the specified waiting time elapsed.

Unknown types

Displays the number data packets with an unknown data type that the device received from the server on the authentication port.

Packets dropped

Displays the number of data packets that the device received from the server on the authentication port and then discarded them.
4.4.5 RADIUS Accounting Statistics

This dialog displays information about the communication between the device and the accounting server. The table displays the information for each server in a separate table row.

To delete the statistic, click in the Network Security > RADIUS > Global dialog the button.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Name**

Displays the name of the server.

**Address**

Displays the IP address of the server.

**Round trip time**

Displays the time interval in hundredths of a second between the last response received from the server (Accounting Response) and the corresponding data packet sent (Accounting Request).

**Accounting-request packets**

Displays the number of accounting request data packets that the device sent to the server. This value does not take repetitions into account.

**Retransmitted accounting-request packets**

Displays the number of accounting request data packets that the device retransmitted to the server.

**Received packets**

Displays the number of accounting response data packets that the device received from the server.

**Malformed packets**

Displays the number of malformed accounting response data packets that the device received from the server (including data packets with an invalid length).

**Bad authenticators**

Displays the number of accounting response data packets with an invalid authenticator that the device received from the server.
Pending requests

Displays the number of accounting request data packets that the device sent to the server to which it has not yet received a response from the server.

Timeouts

Displays how many times no response to the server was received before the specified waiting time elapsed.

Unknown types

Displays the number of data packets with an unknown data type that the device received from the server on the accounting port.

Packets dropped

Displays the number of data packets that the device received from the server on the accounting port and then discarded them.

### 4.5 DoS

Denial of Service (DoS) is a cyber-attack that aims to bring down specific services or devices. In this dialog you can set up several filters to help protect the device itself and other devices in the network from DoS attacks.

The menu contains the following dialogs:

- DoS Global
4.5.1 **DoS Global**

In this dialog you specify the DoS settings for the TCP/UDP, IP and ICMP protocols.

**Note:** We recommend activating the filters to increase the level of security of the device.

**TCP/UDP**

A scanner uses port scans to prepare network attacks. The scanner uses different techniques to determine running devices and open ports. This frame lets you activate filters for specific scanning techniques.

The device supports the detection of the following scan types:
- Null scans
- Xmas scans
- SYN/FIN scans
- TCP Offset attacks
- TCP SYN attacks
- L4 Port attacks
- Minimal Header scans

**Null Scan filter**

Activates/deactivates the Null Scan filter.

The device detects and discards incoming TCP packets with the following properties:
- No TCP flags are set.
- The TCP sequence number is 0.

Possible values:
- **marked**
  - The filter is active.
- **unmarked** *(default setting)*
  - The filter is inactive.

**Xmas filter**

Activates/deactivates the Xmas filter.

The device detects and discards incoming TCP packets with the following properties:
- The TCP flags *FIN, URG* and *PSH* are simultaneously set.
- The TCP sequence number is 0.

Possible values:
- **marked**
  - The filter is active.
- **unmarked** *(default setting)*
  - The filter is inactive.
SYN/FIN filter

Activates/deactivates the SYN/FIN filter.

The device detects incoming data packets with the TCP flags SYN and FIN set simultaneously and discards them.

Possible values:

- **marked**
  The filter is active.
- **unmarked** (default setting)
  The filter is inactive.

TCP Offset protection

Activates/deactivates the TCP Offset protection.

The TCP Offset protection detects incoming TCP data packets whose fragment offset field of the IP header is equal to 1 and discards them.

The TCP Offset protection accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1.

Possible values:

- **marked**
  The protection is active.
- **unmarked** (default setting)
  The protection is inactive.

TCP SYN protection

Activates/deactivates the TCP SYN protection.

The TCP SYN protection detects incoming data packets with the TCP flag SYN set and a L4 source port < 1024 and discards them.

Possible values:

- **marked**
  The protection is active.
- **unmarked** (default setting)
  The protection is inactive.

L4 Port protection

Activates/deactivates the L4 Port protection.

The L4 Port protection detects incoming TCP and UDP data packets whose source port number and destination port number are identical and discards them.

Possible values:

- **marked**
  The protection is active.
- **unmarked** (default setting)
  The protection is inactive.
Min. Header Size filter

Activates/deactivates the Minimal Header filter.

The Minimal Header filter compares the TCP header of incoming data packets. If the data offset value multiplied by 4 is smaller than the minimum TCP header size, then the filter discards the data packet.

Possible values:
- **marked**
  - The filter is active.
- **unmarked** (default setting)
  - The filter is inactive.

Min. TCP header size

Displays the minimum size of a valid TCP header.

IP

Land Attack filter

Activates/deactivates the **Land Attack** filter. With the **Land Attack** method, the attacking station sends data packets whose source and destination addresses are identical to the IP address of the recipient.

Possible values:
- **marked**
  - The filter is active. The device discards data packets whose source and destination addresses are identical.
- **unmarked** (default setting)
  - The filter is inactive.

ICMP

This dialog provides you with filter options for the following ICMP parameters:
- Fragmented data packets
- ICMP packets from a specific size upwards

Fragmented packets filter

Activates/deactivates the filter for fragmented ICMP packets.

The filter detects fragmented ICMP packets and discards them.

Possible values:
- **marked**
  - The filter is active.
- **unmarked** (default setting)
  - The filter is inactive.
Packet size filter

Activates/deactivates the filter for incoming ICMP packets.

The filter detects ICMP packets whose payload size exceeds the size specified in the Allowed payload size [byte] field and discards them.

Possible values:
- marked
  The filter is active.
- unmarked (default setting)
  The filter is inactive.

Allowed payload size [byte]

Specifies the maximum allowed payload size of ICMP packets in bytes.

Mark the Packet size filter checkbox if you want the device to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets.

Possible values:
- 0..1472 (default setting: 512)

4.6 ACL

In this menu, you specify the settings for the Access Control Lists (ACL). Access Control Lists contain rules which the device applies successively to the data stream on its ports or VLANs.

If a data packet matches the criteria of one or more rules, then the device applies the action specified in the first rule that matches to the data stream. The device ignores the rules that follow the first rule that matches. Possible actions include:
- permit: The device forwards the data packet to a port or to a VLAN.
- deny: The device drops the data packet.

In the default setting, the device forwards every data packet. Once you assign an Access Control List to a port or VLAN, then this behavior changes. The device enters at the end of an Access Control List an implicit Deny-All rule. Consequently, the device discards data packets that do not match the criteria of any rules. If you want a different behavior, then add a Permit-All rule at the end of your Access Control Lists.

Proceed as follows to set up Access Control Lists and rules:
- Make a rule and specify the rule settings. See the Network Security > ACL > IPv4 Rule dialog, or the Network Security > ACL > MAC Rule dialog.
- Assign the Access Control List to the ports and VLANs of the device. See the Network Security > ACL > Assignment dialog.

The menu contains the following dialogs:
- ACL IPv4 Rule
- ACL MAC Rule
- ACL Assignment
4.6.1 **ACL IPv4 Rule**

In this dialog you specify the rules that the device applies to the IP data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device lets you filter according to the following criteria:
- Source or destination IP address of a data packet
- Type of the transmitting protocol
- Source or destination port of a data packet

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  Opens the *Create* window to add a table row.
  - In the *Group name* field, you specify the name of the Access Control List to which the rule belongs. When you add a new name, click the + icon.
  - In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first.

- **Remove**
  Removes the selected table row.

**Group name**

Displays the name of the Access Control List. The Access Control List contains the rules.

**Index**

Displays the number of the rule within the Access Control List. You specify the index number when you add a table row.

If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.
Match every packet

Specifies to which IP data packets the device applies the rule.

Possible values:
- **marked** (default setting)
  The device applies the rule to every IP data packet.
- **unmarked**
  The device applies the rule to IP data packets depending on the value in the following fields:
  - Source IP address, Destination IP address, Protocol
  - DSCP, TOS priority, TOS mask
  - Packet fragmented

Source IP address

Specifies the source address of the IP data packets to which the device applies the rule.

Possible values:
- **?.?.?.?** (default setting)
  The device applies the rule to IP data packets with any source address.
- **Valid IPv4 address**
  The device applies the rule to IP data packets with the specified source address.
  You use the ? character as a wild card.
  Example **192.?.?.32**: The device applies the rule to IP data packets whose source address begins with 192. and ends with .32.
- **Valid IPv4 address/bit mask**
  The device applies the rule to IP data packets with the specified source address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example **192.168.1.0/0.0.0.127**: The device applies the rule to IP data packets with a source address in the range from 192.168.1.0 to ….127.

Destination IP address

Specifies the destination address of the IP data packets to which the device applies the rule.

Possible values:
- **?.?.?.?** (default setting)
  The device applies the rule to IP data packets with any destination address.
- **Valid IPv4 address**
  The device applies the rule to data packets with the specified destination address.
  You use the ? character as a wild card.
  Example **192.?.?.32**: The device applies the rule to IP data packets whose source address begins with 192. and ends with .32.
- **Valid IPv4 address/bit mask**
  The device applies the rule to data packets with the specified destination address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example **192.168.1.0/0.0.0.127**: The device applies the rule to IP data packets with a destination address in the range from 192.168.1.0 to ….127.
Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets with a Protocol field of the specified value.

Possible values:
- **any** (default setting)
  - The device applies the rule to every IP data packet without evaluating the protocol type.
- **icmp**
  - Internet Control Message Protocol (RFC 792)
- **igmp**
  - Internet Group Management Protocol
- **ip-in-ip**
  - IP in IP tunneling (RFC 2003)
- **tcp**
  - Transmission Control Protocol (RFC 793)
- **udp**
  - User Datagram Protocol (RFC 768)
- **ip**
  - Internet Protocol

Source TCP/UDP port

Specifies the source port of the IP data packets to which the device applies the rule. The prerequisite is that in the Protocol column the value TCP or UDP is specified.

Possible values:
- **any** (default setting)
  - The device applies the rule to every IP data packet without evaluating the source port.
- **1..65535**
  - The device applies the rule only to IP data packets containing the specified source port.

Destination TCP/UDP port

Specifies the destination port of the IP data packets to which the device applies the rule. The prerequisite is that in the Protocol column the value TCP or UDP is specified.

Possible values:
- **any** (default setting)
  - The device applies the rule to every IP data packet without evaluating the destination port.
- **1..65535**
  - The device applies the rule only to IP data packets containing the specified destination port.

Action

Specifies how the device processes received IP data packets when the device applies the rule.

Possible values:
- **permit** (default setting)
  - The device forwards the IP data packets.
- **deny**
  - The device drops the IP data packets.
Log

Activates/deactivates the logging in the log file. See the Diagnostics > Report > System Log dialog.

Possible values:

- **marked**
  - Logging is active.
  - The prerequisite is that in the Network Security > ACL > Assignment dialog the Access Control List is assigned to a VLAN or port.
  - The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to IP data packets.

- **unmarked** (default setting)
  - Logging is inactive.

The device lets you activate this function for up to 128 deny rules.
4.6.2 **ACL MAC Rule**

In this dialog you specify the rules that the device applies to the MAC data packets.

An Access Control List (group) contains one or more rules. The device applies the rules of an Access Control List successively, beginning with the rule with the lowest value in the *Index* column.

The device lets you filter according to the following criteria:

> Source or destination MAC address of a data packet

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  
  Opens the *Create* window to add a table row.
  
  - In the *Group name* field, you specify the name of the Access Control List to which the rule belongs. When you add a new name, click the icon.
  
  - In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first.

- **Remove**

  Removes the selected table row.

**Group name**

Displays the name of the Access Control List. The Access Control List contains the rules.

**Index**

Displays the number of the rule within the Access Control List. You specify the index number when you add a table row.

If the Access Control List contains multiple rules, then the device processes the rule with the lowest value first.
Match every packet

Specifies to which MAC data packets the device applies the rule.

Possible values:

- **marked** (default setting)
  The device applies the rule to every MAC data packet.

- **unmarked**
  The device applies the rule to MAC data packets depending on the value in the following fields:
  - *Source MAC address*
  - *Destination MAC address*

Source MAC address

Specifies the source address of the MAC data packets to which the device applies the rule.

Possible values:

- **??::??::??::??::??::??** (default setting)
  The device applies the rule to MAC data packets with any source address.

- **Valid MAC address**
  The device applies the rule to MAC data packets with the specified source address.
  You use the `?` character as a wild card.
  Example 00:11:??:??:??:??:??:??:??:??:??: The device applies the rule to MAC data packets whose source address begins with 00:11.

- **Valid MAC address/bit mask**
  The device applies the rule to MAC data packets with the specified source address. The bit mask lets you specify the address range with bit-level accuracy.
  Example 00:11:22:54:??:??:??:??:??:??:??: The device applies the rule to MAC data packets with a source address in the range from 00:11:22:54 to 00:11:22:57.

Destination MAC address

Specifies the destination address of the MAC data packets to which the device applies the rule.

Possible values:

- **??::??::??::??::??::??** (default setting)
  The device applies the rule to MAC data packets with any destination address.

- **Valid MAC address**
  The device applies the rule to MAC data packets with the specified destination address.
  You use the `?` character as a wild card.
  Example 00:11:??:??:??:??:??:??:??:??:??: The device applies the rule to MAC data packets whose destination address begins with 00:11.

- **Valid MAC address/bit mask**
  The device applies the rule to MAC data packets with the specified destination address. The bit mask lets you specify the address range with bit-level accuracy.
  Example 00:11:22:54:??:??:??:??:??:??:??: The device applies the rule to MAC data packets with a destination address in the range from 00:11:22:54 to 00:11:22:57.
Action

Specifies how the device processes received MAC data packets when the device applies the rule.

Possible values:
- **permit** (default setting)
  The device forwards the MAC data packets.
- **deny**
  The device discards the MAC data packets.

Log

Activates/deactivates the logging in the log file. See the Diagnostics > Report > System Log dialog.

Possible values:
- **marked**
  Logging is active.
  The prerequisite is that in the Network Security > ACL > Assignment dialog the Access Control List is assigned to a VLAN or port.
  The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets.
- **unmarked** (default setting)
  Logging is inactive.

The device lets you activate this function for up to 128 deny rules.
4.6.3 ACL Assignment

This dialog lets you assign one or more Access Control Lists to the ports and VLANs of the device. By assigning a priority you specify the processing sequence, provided you assign one or more Access Control Lists to a port or VLAN.

The device applies rules successively, namely in the sequence specified by the rule index. You specify the priority of a group in the Priority column. The lower the number, the higher the priority. In this process, the device applies the rules with a high priority before the rules with a low priority.

The assignment of Access Control Lists to ports and VLANs results in the following different types of ACLs:
- Port-based IPv4 ACLs
- Port-based MAC ACLs
- VLAN-based IPv4 ACLs
- VLAN-based MAC ACLs

The device lets you apply the Access Control Lists to data packets received (inbound).

Note: Before you enable the function, verify that at least one active table row in the table lets you access. Otherwise, the connection to the device terminates if you change the settings. To access the device management is possible only using the CLI through the serial interface of the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Opens the Create window to assign a rule to a port or a VLAN.
• In the Port/VLAN field, you specify the number of the port or the VLAN ID to which the device applies the rule.
• In the Priority field, you specify the sequence in which the device applies the rules to the data stream.
• In the Direction field, you specify if the device applies the rule to data packets received or sent.
• In the Group name field, you specify which rule the device assigns to the port or VLAN.

Remove

Removes the selected table row.

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.
Network Security

Network Security > ACL > Assignment

Type

Displays if the Access Control List contains MAC rules or IPv4 rules.

Possible values:

- **mac**
  The Access Control List contains MAC rules.

- **ip**
  The Access Control List contains IPv4 rules.


Port

Displays the port to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a VLAN.

VLAN ID

Displays the VLAN to which the Access Control List is assigned. The field remains empty when the Access Control List is assigned to a port.

Direction

Displays that the device applies the Access Control List to received data packets.

Priority

Displays the priority of the Access Control List.

Using the priority, you specify the sequence in which the device applies the Access Control Lists to the data stream. The device applies the rules in ascending order which starts with priority 1. If an Access Control List is assigned to a port and to a VLAN with the same priority, then the device applies the rules to the port first.

Possible values:

- 1..4294967295

Active

Displays if the Access Control List on the port or in the VLAN is active.

Possible values:

- **marked** (default setting)
  The Access Control List is active.

- **unmarked**
  The Access Control List is inactive.
5 Switching

The menu contains the following dialogs:
- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundancy

5.1 Switching Global

This dialog lets you specify the following settings:
- Change the Aging time of the address table
- Enable the flow control in the device
- Activate the VLAN-unaware mode function

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.
- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

Then the connected devices do not send any more data packets for as long as the signaling takes. On uplink ports, this can possibly cause undesired sending breaks in the higher-level network segment (“wandering backpressure”). The flow control mechanism thus slows down the network to the bandwidth that the slowest device in the network can process.

According to standard IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN \(\geq 1\). However, a small number of applications on connected end devices send or receive data packets with a VLAN ID=0. Data packets with a VLAN ID=0 are called Priority Tagged Frames. When the device receives one of these data packets, before forwarding it the device overwrites the original value in the data packet with the VLAN ID of the receiving port.

If you activate the VLAN-unaware mode function, then this deactivates the VLAN settings in the device. The device then transparently forwards the data packets and evaluates the priority information contained only in the data packet.
**Configuration**

**MAC address**

Displays the MAC address of the device.

**Aging time [s]**

Specifies the aging time in seconds.

Possible values:

- **10..500000** (default setting: **30**)

The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its address table.

You find the address table in the *Switching > Filter for MAC Addresses* dialog.

**Flow control**

Activates/deactivates the flow control in the device.

Possible values:

- **marked**
  - The flow control is active in the device.
  - Additionally activate the flow control on the required ports. See the *Basic Settings > Port* dialog, *Configuration* tab, checkbox in the *Flow control* column.

- **unmarked** (default setting)
  - The flow control is inactive in the device.

If you are using a redundancy function, then deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

**VLAN-unaware mode**

Activates/deactivates the mode in which the device ignores the VLAN ID and forwards the data packets unchanged. The device continues to evaluate the priority information in the data packets.

On the connected end devices, only some applications require receiving data packets with a VLAN ID=0. If applications in your network require this, then activate the function.

Possible values:

- **marked**
  - The device operates in the *VLAN-unaware* mode based on the IEEE 802.1Q specification:
    - The device ignores the VLAN settings in the device and the VLAN ID in the data packets.
    - The device transmits the data packets based on their destination MAC address.
    - The device evaluates the priority information contained in the VLAN tag of the data packets.
    - The device ignores the VLAN settings specified in the *Switching > VLAN > Configuration* and *Switching > VLAN > Port* dialogs.
**Note:** You specify the VLAN ID for every function in the device which uses VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping.

- **unmarked** (default setting)
  The device operates in the VLAN-aware mode based on the IEEE 802.1Q specification:
  - The device evaluates the VLAN tags in the data packets.
  - The device transmits the data packets based on their destination MAC address or destination IP address in the corresponding VLAN.
  - The device evaluates the priority information contained in the data packet.
  - When the device receives a data packet with VLAN ID=0 it assigns the VLAN ID of the port to the data packet. See the *Switching > VLAN > Port* dialog.
5.2 Rate Limiter

The device lets you limit the amount of data packets on the ports to help provide stable operation even with a large data volume. If the amount of data packets on a port exceed the threshold value, then the device discards the excess data packets on this port.

The rate limiter function operates only on Layer 2, and is used to limit the effects of storms of data packets that flood the device (typically Broadcasts).

The rate limiter function ignores protocol information on higher layers, such as IP or TCP.

The dialog contains the following tabs:
- [Ingress]
- [Egress]

**[Ingress]**

In this tab you enable the Rate Limiter function. The threshold value specifies the maximum amount of data packets the port receives. If the amount of data packets on a port exceed the specified threshold value, then the device discards the excess data packets on this port.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>Specifies the threshold value for broadcast, multicast, and unicast data packets on this port:</td>
</tr>
</tbody>
</table>

Possible values:
- 0 (default setting)
  - The Rate Limiter function is deactivated on this port.
- 1..24414 at 100 MBit/s
- 1..244140 at 1000 MBit/s
- If the value percent is specified in the Threshold unit column, then specify a percentage value between 1 and 100.
- If the value pps is specified in the Threshold unit column, then specify an absolute value.
  - The rate limiter function calculates the threshold based on 512-byte-sized packets.

**Note:** The operating modes actually available depend on the device hardware and the media module used.
Threshold unit

Specifies the unit for the threshold value:

Possible values:
- **percent** (default setting)
  Specifies the threshold value as a percentage of the data rate of the port.
- **pps**
  Specifies the threshold value in data packets per second.

Broadcast mode

Activates/deactivates the rate limiter function for received broadcast data packets.

Possible values:
- **marked**
- **unmarked** (default setting)

If the threshold value is exceeded, then the device discards the excess broadcast data packets on this port.

Multicast mode

Activates/deactivates the rate limiter function for received multicast data packets.

Possible values:
- **marked**
- **unmarked** (default setting)

If the threshold value is exceeded, then the device discards the excess multicast data packets on this port.

Unknown unicast mode

Activates/deactivates the rate limiter function for received unicast data packets with an unknown destination address.

Possible values:
- **marked**
- **unmarked** (default setting)

If the threshold value is exceeded, then the device discards the excess unicast data packets on this port.

**[Egress]**

In this tab you specify the egress transmission rate on the port.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Bandwidth [%]

Specifies the egress transmission rate.

Possible values:

- **0** (default setting)
  - The bandwidth limitation is disabled.
- **1..100**
  - The bandwidth limitation is enabled.
  - This value specifies the percentage of overall link speed for the port in 1% increments.
5.3 Filter for MAC Addresses

This dialog lets you display and edit address filters for the address table. Address filters specify the way the data packets are forwarded in the device based on the destination MAC address.

Each table row represents one filter. The device automatically sets up the filters. The device lets you set up additional filters manually.

The device transmits the data packets as follows:
- When the table contains the destination address of a data packet, the device transmits the data packet from the receiving port to the port specified in the table row.
- When there is no table entry for the destination address, the device transmits the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the address table, click in the Basic Settings > Restart dialog the Reset MAC address table button.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add
Opens the Create window to add a table row.
- In the Address field, you specify the destination MAC address.
- In the VLAN ID field, you specify the ID of the VLAN.
- In the Port field, you specify the port.
  - Select one port if the destination MAC address is a unicast address.
  - Select one or more ports if the destination MAC address is a multicast address.
  - Select no port to create a discard filter. The device discards data packets with the destination MAC address specified in the table entry.

Remove
Removes the selected table row.

Reset MAC address table
Removes the MAC addresses from the forwarding table that have the value learned in the Status column.

Address
Displays the destination MAC address to which the table row applies.
VLAN ID

Displays the ID of the VLAN to which the table row applies.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

Status

Displays how the device has set up the address filter.

Possible values:

- **learned**
  Address filter set up automatically by the device based on received data packets.

- **mgmt**
  MAC address of the device. The address filter is protected against changes.

- **other**
  Static address added by a security protocol, for example by the 802.1X or Port Security function.

- **permanent**
  Address filter set up manually. The address filter stays set up permanently.

- **GMRP**
  Multicast address filter automatically set up by GMRP.

- **IGMP**
  Address filter automatically set up by IGMP Snooping.

- **MRP-MMRP**
  Multicast address filter automatically set up by MMRP.

<Port number>

Displays how the corresponding port transmits data packets which it directs to the adjacent destination address.

Possible values:

- **-**
  The port does not transmit any data packets to the destination address.

- **learned**
  The port transmits data packets to the destination address. The device created the filter automatically based on received data packets.

- **IGMP learned**
  The port transmits data packets to the destination address. The device created the filter automatically based on IGMP.

- **unicast static**
  The port transmits data packets to the destination address. A user created the filter.

- **multicast static**
  The port transmits data packets to the destination address. A user created the filter.
5.4 **IGMP Snooping**

The Internet Group Management Protocol (IGMP) is a protocol for dynamically managing Multicast groups. The protocol describes the distribution of Multicast data packets between routers and end devices on Layer 3.

The device lets you use the IGMP Snooping function to also use the IGMP mechanisms on Layer 2:
- Without IGMP Snooping, the device transmits the Multicast data packets to every port.
- With the activated IGMP Snooping function, the device transmits the Multicast data packets only on ports to which Multicast receivers are connected. This reduces the network load. The device evaluates the IGMP data packets transmitted on Layer 3 and uses the information on Layer 2.

Activate the IGMP Snooping function not until the following conditions are fulfilled:
- There is a Multicast router in the network that creates IGMP queries (periodic queries).
- The devices participating in IGMP Snooping forward the IGMP queries.

The device links the IGMP reports with the entries in its address table. When a multicast receiver joins a multicast group, the device creates a table row for this port in the Switching > Filter for MAC Addresses dialog. When the multicast receiver leaves the multicast group, the device removes the table row.

The menu contains the following dialogs:
- IGMP Snooping Global
- IGMP Snooping Configuration
- IGMP Snooping Enhancements
- IGMP Snooping Querier
- IGMP Snooping Multicasts
5.4.1 IGMP Snooping Global

This dialog lets you enable the IGMP Snooping protocol in the device and also configure it for each port and each VLAN.

Operation

Enables/disables the IGMP Snooping function in the device.

Possible values:

- **On**: The IGMP Snooping function is enabled in the device according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

- **Off** (default setting): The IGMP Snooping function is disabled in the device. The device transmits received query, report, and leave data packets without evaluating them. Received data packets with a Multicast destination address are transmitted to every port by the device.

Information

Buttons

- Reset IGMP snooping counters

Removes the IGMP Snooping entries and resets the counter in the Information frame to 0.

Multicast control packets processed

Displays the number of Multicast control data packets processed.

This statistic encompasses the following packet types:

- IGMP Reports
- IGMP Queries version V1
- IGMP Queries version V2
- IGMP Queries version V3
- IGMP Queries with an incorrect version
- PIM or DVMRP packets

The device uses the Multicast control data packets to create the address table for transmitting the Multicast data packets.
Possible values:

- $0..2^{31}-1$

You use the *Reset IGMP snooping data* button in the *Basic Settings > Restart* dialog or the command `clear igmp-snooping` using the Command Line Interface to reset the IGMP Snooping entries, including the counter for the processed multicast control data packets.
5.4.2 IGMP Snooping Configuration

This dialog lets you enable the IGMP Snooping function in the device and also configure it for each port and each VLAN.

The dialog contains the following tabs:
- [VLAN ID]
- [Port]

[VLAN ID]

In this tab you configure the IGMP Snooping function for every VLAN.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

VLAN ID

Displays the ID of the VLAN to which the table row applies.

Active

Activates/deactivates the IGMP Snooping function for this VLAN.

The prerequisite is that the IGMP Snooping function is globally enabled.

Possible values:
- marked
  IGMP Snooping is activated for this VLAN. The VLAN has joined the Multicast data stream.
- unmarked (default setting)
  IGMP Snooping is deactivated for this VLAN. The VLAN has left the Multicast data stream.

Group membership interval

Specifies the time in seconds for which a VLAN from a dynamic Multicast group remains entered in the address table when the device does not receive any more report data packets from the VLAN.

Specify a value larger than the value in the Max. response time column.
Possible values:
➢ 2..3600  (default setting: 260)

Max. response time

Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Specify a value smaller than the value in the Group membership interval column.

Possible values:
➢ 1..25  (default setting: 10)

Fast leave admin mode

Activates/deactivates the Fast Leave function for this VLAN.

Possible values:
➢ marked
  When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
➢ unmarked  (default setting)
  When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a VLAN does not send any more report messages.

MRP expiration time

Multicast Router Present Expiration Time. Specifies the time in seconds for which the device waits for a query on this port that belongs to a VLAN. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

You have the option of configuring this parameter only if the port belongs to an existing VLAN.

Possible values:
➢ 0
  unlimited timeout - no expiration time
➢ 1..3600  (default setting: 260)

[Port]

In this tab you configure the IGMP Snooping function for every port.
Switching
[Switching > IGMP Snooping > Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Active

Activates/deactivates the IGMP Snooping function on the port.

The prerequisite is that the IGMP Snooping function is globally enabled.

Possible values:

- **marked**
  IGMP Snooping is active on this port. The device includes the port in the multicast data stream.

- **unmarked** (default setting)
  IGMP Snooping is inactive on this port. The port left the multicast data stream.

Group membership interval

Specifies the time in seconds for which a port, from a dynamic multicast group, remains entered in the address table when the device does not receive any more report data packets from the port.

Possible values:

- **2..3600** (default setting: 260)
  Specify the value larger than the value in the Max. response time column.

Max. response time

Specifies the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. You thus help prevent the multicast group members from responding to the query at the same time.

Possible values:

- **1..25** (default setting: 10)
  Specify a value lower than the value in the Group membership interval column.

MRP expiration time

Specifies the Multicast Router Present Expiration Time. The MRP expiration time is the time in seconds for which the device waits for a query packet on this port. When the port does not receive a query data packet, the device removes the port from the list of ports with connected multicast routers.

Possible values:

- **0**
  unlimited timeout - no expiration time

- **1..3600** (default setting: 260)
Fast leave admin mode

Activates/deactivates the Fast Leave function on the port.

Possible values:
- marked
  When the Fast Leave function is active and the device receives an IGMP Leave message from a multicast group, the device immediately removes the entry from its address table.
- unmarked (default setting)
  When the Fast Leave function is inactive, the device first sends MAC-based queries to the members of the multicast group and removes an entry when a port does not send any more report messages.

Static query port

Activates/deactivates the Static query port mode.

Possible values:
- marked
  The Static query port mode is active.
  The port is a static query port in the VLANs that are set up.
- unmarked (default setting)
  The Static query port mode is inactive.
  The port is not a static query port. The device transmits IGMP report messages to the port only if it receives IGMP queries.

VLAN IDs

Displays the ID of the VLANs to which the table row applies.
5.4.3 IGMP Snooping Enhancements

This dialog lets you select a port for a VLAN ID and to configure the port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Wizard

Opens the Wizard window that helps you select and set up the ports. See “[Wizard: IGMP snooping enhancements]” on page 185.

VLAN ID

Displays the ID of the VLAN to which the table row applies.

<Port number>

Displays for every VLAN set up in the device if the relevant port is a query port. Additionally, the field displays if the device transmits every Multicast stream in the VLAN to this port.

Possible values:

- The port is not a query port in this VLAN.
- Learned
  The device detected the port as a query port because the port received IGMP queries in this VLAN. The port is not a statically configured query port.
- Automatic
  The device detected the port as a query port. The prerequisite is that you configure the port as Learn by LLDP.
- Static (manual setting)
  A user specified the port as a static query port. The device transmits IGMP reports only to ports on which it previously received IGMP queries – and to statically configured query ports.

To assign this value, perform the following steps:

- Open the Wizard window.
- On the Configuration page, mark the Static checkbox.
Switching

RM GUI GRS HiOS-2A
Release 9.1 08/2022

185

P= Learn by LLDP (manual setting)
A user specified the port as Learn by LLDP.
With the Link Layer Discovery Protocol (LLDP), the device detects Hirschmann devices connected directly to the port. The device denotes the detected query ports with $A$.
To assign this value, perform the following steps:
☐ Open the Wizard window.
☐ On the Configuration page, mark the Learn by LLDP checkbox.

F= Forward All (manual setting)
A user specified the port so that the device transmits every received Multicast stream in the VLAN to this port. Use this setting for diagnostics purposes, for example.
To assign this value, perform the following steps:
☐ Open the Wizard window.
☐ On the Configuration page, mark the Forward all checkbox.

Display categories

- **Learned (L)**
The table displays cells which contain the value $L$ and possibly further values. Cells which contain other values than $L$ only, the table displays with the “-” symbol.

- **Static (S)**
The table displays cells which contain the value $S$ and possibly further values. Cells which contain other values than $S$ only, the table displays with the “-” symbol.

- **Automatic (A)**
The table displays cells which contain the value $A$ and possibly further values. Cells which contain other values than $A$ only, the table displays with the “-” symbol.

- **Learned by LLDP (P)**
The table displays cells which contain the value $P$ and possibly further values. Cells which contain other values than $P$ only, the table displays with the “-” symbol.

- **Forward all (F)**
The table displays cells which contain the value $F$ and possibly further values. Cells which contain other values than $F$ only, the table displays with the “-” symbol.

**Wizard: IGMP snooping enhancements**

The Wizard window helps you select and configure the ports.

The Wizard window guides you through the following steps:
- **Selection VLAN/Port**
- **Configuration**

After closing the Wizard window, click the ✓ button to save your settings.

**Selection VLAN/Port**

VLAN ID

Select the ID of the VLAN.
Port

Select the ports.

Configuration

VLAN ID

Displays the ID of the selected VLAN.

Port

 Displays the number of the selected ports.

Static

Specifies the port as static query port in the VLANs that are set up. The device transmits IGMP report messages to the ports at which it receives IGMP queries. This lets you also transmit IGMP report messages to other selected ports or connected Hirschmann devices (Automatic).

Learn by LLDP

 Specifies the port as Learn by LLDP. Lets the device detect directly connected Hirschmann devices using LLDP and learn the related ports as a query port.

Forward all

Specifies the port as Forward all. With the Forward all setting, the device transmits at this port every data packet with a Multicast address in the destination address field.
5.4.4 IGMP Snooping Querier

The device lets you send a Multicast stream only to those ports to which a Multicast receiver is connected.

To determine which ports Multicast receivers are connected to, the device sends query data packets to the ports at a definable interval. When a Multicast receiver is connected, it joins the Multicast stream by responding to the device with a report data packet.

This dialog lets you configure the Snooping Querier settings globally and for the VLANs that are set up.

**Operation**

Enables/disables the IGMP Querier function globally in the device.

Possible values:
- **On**
- **Off** (default setting)

**Configuration**

In this frame you specify the IGMP Snooping Querier settings for the general query data packets.

**Protocol version**

Specifies the IGMP version of the general query data packets.

Possible values:
- **1** (IGMP v1)
- **2** (default setting) (IGMP v2)
- **3** (IGMP v3)
Query interval [s]

Specifies the time in seconds after which the device generates general query data packets itself when it has received query data packets from the Multicast router.

Possible values:
- 1..1800 (default setting: 60)

Expire interval [s]

Specifies the time in seconds after which an active querier switches from the passive state back to the active state if it has not received any query packets for longer than specified here.

Possible values:
- 60..300 (default setting: 125)

**Table**

In the table you specify the Snooping Querier settings for the VLANs that are set up.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Displays the ID of the VLAN to which the table row applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activates/deactivates the IGMP Snooping Querier function for this VLAN.</td>
</tr>
<tr>
<td>Current state</td>
<td>Displays if the Snooping Querier is active for this VLAN.</td>
</tr>
</tbody>
</table>

**Possible values:**
- marked
  - The IGMP Snooping Querier function is active for this VLAN.
- unmarked (default setting)
  - The IGMP Snooping Querier function is inactive for this VLAN.

- marked
  - The Snooping Querier is active for this VLAN.
- unmarked
  - The Snooping Querier is inactive for this VLAN.
Address

Specifies the IP address that the device adds as the source address in generated general query data packets. You use the address of the multicast router.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Protocol version

Displays the IGMP protocol version of the general query data packets.

Possible values:
- 1  IGMP v1
- 2  (default setting)  IGMP v2
- 3  IGMP v3

Max. response time

Displays the time in seconds in which the members of a Multicast group respond to a query data packet. For their response, the members specify a random time within the response time. This helps prevent every Multicast group member to respond to the query at the same time.

Last querier address

Displays the IP address of the Multicast router from which the last received IGMP query was sent out.

Last querier version

Displays the IGMP version that the Multicast router used when sending out the last IGMP query received in this VLAN.
5.4.5 IGMP Snooping Multicasts

The device lets you specify how it transmits data packets with unknown Multicast addresses: Either the device discards these data packets, floods them to every port, or transmits them only to the ports that previously received query packets.

The device also lets you transmit the data packets with known Multicast addresses to the query ports.

Configuration

Unknown multicasts

Specifies how the device forwards data packets with unknown Multicast addresses.

Possible values:

- **discard**
  The device discards data packets with an unknown MAC/IP Multicast address.

- **flood** (default setting)
  The device forwards data packets with an unknown MAC/IP Multicast address to every port.

- **query ports**
  The device forwards data packets with an unknown MAC/IP Multicast address to the query ports.

Table

In the table you specify the settings for known Multicasts for the VLANs that are set up.

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

VLAN ID

Displays the ID of the VLAN to which the table row applies.

Known multicasts

Specifies how the device forwards data packets with known Multicast addresses.

Possible values:

- **send to query and registered ports**
  The device forwards data packets with a known MAC/IP Multicast address to the query ports and to the registered ports.

- **send to registered ports** (default setting)
  The device forwards data packets with a known MAC/IP Multicast address to registered ports.
5.5 **MRP-IEEE**

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP). The Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP) replace these protocols.

MRP-IEEE helps confine traffic to the required areas of the LAN. To confine traffic, the MRP-IEEE applications distribute attribute values to participating MRP-IEEE devices across a LAN registering and de-registering multicast group membership and VLAN identifiers.

Registering group participants lets you reserve resources for specific data packets transversing a LAN. Defining resource requirements regulates the level of traffic, allowing the devices to determine the required resources and provides for dynamic maintenance of the allocated resources.

The menu contains the following dialogs:
- MRP-IEEE Configuration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol
5.5.1 MRP-IEEE Configuration

This dialog lets you set the various MRP timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdraws and re-registrations. The default timer values effectively maintain these relationships.

When you reconfigure the timers, maintain the following relationships:
► To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, specify the LeaveTime to: \( \geq (2 \times \text{JoinTime}) + 60 \).
► To minimize the volume of rejoining data packets generated following a LeaveAll event, specify the value for the LeaveAll timer larger than the LeaveTime value.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join time [1/100s]</td>
<td>Specifies the Join timer which controls the interval between transmit opportunities applied to the Applicant state machine.</td>
</tr>
<tr>
<td>Possible values:</td>
<td>► 10..100 (default setting: 20)</td>
</tr>
<tr>
<td>Leave time [1/100s]</td>
<td>Specifies the Leave timer which controls the period that the Registrar state machine waits in the leave (LV) state before transiting to the empty (MT) state.</td>
</tr>
<tr>
<td>Possible values:</td>
<td>► 20..600 (default setting: 60)</td>
</tr>
<tr>
<td>Leave all time [1/100s]</td>
<td>Specifies the LeaveAll timer which controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs.</td>
</tr>
<tr>
<td>Possible values:</td>
<td>► 200..6000 (default setting: 1000)</td>
</tr>
</tbody>
</table>
5.5.2 MRP-IEEE Multiple MAC Registration Protocol

The Multiple MAC Registration Protocol (MMRP) lets end devices and MAC switches register and de-register group membership and individual MAC address information with switches located in the same LAN. The switches within the LAN disseminate the information through switches that support extended filtering services. Using the MAC address information, MMRP lets you confine multicast traffic to the required areas of a Layer 2 network.

For an example of how MMRP works, consider a security camera mounted on a mast overlooking a building. The camera sends multicast packets onto a LAN. You have 2 end devices installed for surveillance in separate locations. You register the MAC addresses of the camera and the 2 end devices in the same multicast group. You then specify the MMRP settings on the ports to send the multicast group packets to the 2 end devices.

The dialog contains the following tabs:

- [Configuration]
- [Service requirement]
- [Statistics]

[Configuration]

In this tab you select active MMRP port participants and set the device to transmit periodic events. The dialog also lets you enable VLAN registered MAC address broadcasting.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the devices associated with the active port.

Operation

Enables/disables the global MMRP function in the device. The device participates in MMRP message exchanges.

Possible values:

- **On**
  The device is a normal participant in MMRP message exchanges.

- **Off** (default setting)
  The device ignores MMRP messages.
**Configuration**

Periodic state machine

Enables/disables the global periodic state machine in the device.

Possible values:
- **On**
  With MMRP Operation enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports.
- **Off** (default setting)
  Disables the periodic state machine in the device.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

| Port | Displays the port number. |

Active

Activates/deactivates the port MMRP participation.

Possible values:
- **marked** (default setting)
  With MMRP enabled globally and on this port, the device sends and receives MMRP messages on this port.
- **unmarked**
  Disables the port MMRP participation.

Restricted group registration

Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

Possible values:
- **marked**
  If enabled and a static filter entry for the MAC address exists on the VLAN concerned, then the device registers the MAC address attributes dynamically.
- **unmarked** (default setting)
  Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.
[Service requirement]
This tab contains forwarding parameters for each active VLAN, specifying the ports on which multicast forwarding applies. The device lets you statically setup VLAN ports as Forward all or Forbidden. You set the Forbidden MMRP service requirement statically only through the Graphical User Interface or Command Line Interface.

A port is setup only as ForwardAll or Forbidden.

Table
For information on how to customize the appearance of the table, see “Working with tables” on page 16.

| VLAN ID | Displays the ID of the VLAN. |
| <Port number> | Specifies the service requirement handling for the port. |

Possible values:
- **FA**
  Specifies the ForwardAll traffic setting on the port. The device forwards the data packets destined to MMRP registered multicast MAC addresses on the VLAN. The device forwards the data packets to ports which MMRP has dynamically setup or ports which the administrator has statically setup as ForwardAll ports.
- **F**
  Specifies the Forbidden traffic setting on the port. The device blocks dynamic MMRP ForwardAll service requirements. With ForwardAll requests blocked on this port in this VLAN, the device blocks the data packets destined to MMRP registered multicast MAC addresses on this port. Furthermore, the device blocks MMRP service request for changing this value on this port.
- **-** (default setting)
  Disables the forwarding functions on this port.
- **Learned**
  Displays values setup by MMRP service requests.

[Statistics]
Devices on a LAN exchange Multiple MAC Registration Protocol Data Units (MMRPDUs) to maintain statuses of devices on an active MMRP port. This tab lets you monitor the MMRP data packets statistics for each port.
Switching

[Switching > MRP-IEEE > MMRP]

Information

Buttons

![Reset statistics](image)

Reset statistics

 Resets the port statistics counters and the values in the Last received MAC address column.

Transmitted MMRP PDU

Displays the number of MMRP PDUUs transmitted in the device.

Received MMRP PDU

Displays the number of MMRP PDUUs received in the device.

Received bad header PDU

Displays the number of MMRP PDUUs received with a bad header in the device.

Received bad format PDU

Displays the number of MMRP PDUUs with a bad data field that were not transmitted in the device.

Transmission failed

Displays the number of MMRP PDUUs not transmitted in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Transmitted MMRP PDU

Displays the number of MMRP PDUUs transmitted on the port.

Received MMRP PDU

Displays the number of MMRP PDUUs received on the port.

Received bad header PDU

Displays the number of MMRP PDUUs with a bad header that were received on the port.

Received bad format PDU

Displays the number of MMRP PDUUs with a bad data field that were not transmitted on the port.
Transmission failed

Displays the number of MMRPDUs not transmitted on the port.

Last received MAC address

Displays the last MAC address from which the port received MMRPDUs.
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

The Multiple VLAN Registration Protocol (MVRP) provides a mechanism that lets you distribute VLAN information and configure VLANs dynamically. For example, when you configure a VLAN on an active MVRP port, the device distributes the VLAN information to other MVRP enabled devices. Using the information received, an MVRP enabled device dynamically creates the VLAN trunks on other MVRP enabled devices as needed.

The dialog contains the following tabs:
- [Configuration]
- [Statistics]

[Configuration]

In this tab you select active MVRP port participants and set the device to transmit periodic events.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the VLANs associated with the active port. Using the periodic events, MVRP enabled switches dynamically maintain the VLANs.

Operation

Enables/disables the global Applicant Administrative Control which specifies if the Applicant state machine participates in MMRP message exchanges.

Possible values:
- On
  Normal Participant. The Applicant state machine participates in MMRP message exchanges.
- Off (default setting)
  Non-Participant. The Applicant state machine ignores MMRP messages.
**Configuration**

**Periodic state machine**

Enables/disables the periodic state machine in the device.

Possible values:
- **On**
  The periodic state machine is enabled.
  With MVRP *Operation* enabled globally, the device transmits MVRP periodic events in 1 second intervals, on MVRP participating ports.
- **Off** (default setting)
  The periodic state machine is disabled.
  Disables the periodic state machine in the device.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activates/deactivates the port MVRP participation.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>marked (default setting)</td>
<td>With MVRP <em>Operation</em> enabled globally and on this port, the device distributes VLAN membership information to MVRP-aware devices connected to this port.</td>
</tr>
<tr>
<td>unmarked</td>
<td>Disables the port MVRP participation.</td>
</tr>
<tr>
<td>Restricted VLAN registration</td>
<td>Activates/deactivates the Restricted VLAN registration function on this port.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>marked</td>
<td>If enabled and a static VLAN registration entry exists, then the device lets you create a dynamic VLAN for this entry.</td>
</tr>
<tr>
<td>unmarked (default setting)</td>
<td>Disables the Restricted VLAN registration function on this port.</td>
</tr>
</tbody>
</table>

**Statistics**

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDU) to maintain statuses of VLANs on active ports. This tab lets you monitor the MVRP data packets.
Information

Buttons

- **Reset statistics**

  Resets the port statistics counters and the values in the Last received MAC address column.

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted in the device.

Received MVRP PDU

Displays the number of MVRPDUs received in the device.

Received bad header PDU

Displays the number of MVRPDUs received with a bad header in the device.

Received bad format PDU

Displays the number of MVRPDUs with a bad data field that the device blocked.

Transmission failed

Displays the number of detected failures while adding a message into the MVRP queue.

Message queue failures

Displays the number of MVRPDUs that the device blocked.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted on the port.

Received MVRP PDU

Displays the number of MVRPDUs received on the port.

Received bad header PDU

Displays the number of MVRPDUs with a bad header that the device received on the port.
Received bad format PDU

Displays the number of MVRPDUs with a bad data field that the device blocked on the port.

Transmission failed

Displays the number of MVRPDUs that the device blocked on the port.

Registrations failed

Displays the number of unsuccessful registration attempts on the port.

Last received MAC address

Displays the last MAC address from which the port received MVRPDUs.

5.6 GARP

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and multicast group membership.

When an attribute for a participant is registered or deregistered according to GARP, the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

Note: Before you enable the GMRP function, verify that the MMRP function is disabled.

The menu contains the following dialogs:
- GMRP
- GVRP
5.6.1 GMRP

The GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. GARP also lets the devices distribute the information across the network devices that support extended filtering services.

GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P.

Operation

Enables/disables the global GMRP function in the device. The device participates in GMRP message exchanges.

Possible values:
- **On**: GMRP is enabled.
- **Off** (default setting): The device ignores GMRP messages.

Multicasts

Unknown multicasts

Enables/disables the unknown multicast data to be either flooded or discarded.

Possible values:
- **discard**: The device discards unknown multicast data.
- **flood** (default setting): The device forwards unknown multicast data to every port.

Table

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

Port

Displays the port number.
GMRP active

Activates/deactivates the port GMRP participation.

The prerequisite is that the GMRP function is globally enabled.

Possible values:

- **marked** (default setting)
  - The port GMRP participation is active.

- **unmarked**
  - The port GMRP participation is inactive.

Service requirement

Specifies the ports on which multicast forwarding applies.

Possible values:

- **Forward all unregistered groups** (default setting)
  - The device forwards data destined to GMRP-registered multicast MAC addresses on the VLAN.
  - The device forwards data to the unregistered groups.

- **Forward all groups**
  - The device forwards data destined to every group, registered or unregistered.
5.6.2 GVRP

The GARP VLAN Registration Protocol (GVRP) or Generic VLAN Registration Protocol is a protocol that facilitates control of Virtual Local Area Networks (VLANs) within a larger network. GVRP is a Layer 2 network protocol, used to automatically configure devices in a VLAN network.

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning, and creating dynamic VLAN on 802.1Q trunk ports. With GVRP, the device exchanges VLAN configuration information with other GVRP devices. Thus, the device reduces the unnecessary broadcast and unknown unicast traffic. Exchanging VLAN configuration information also lets you dynamically create and manage VLANs connected through the 802.1Q trunk ports.

Operation

Enables/disables the GVRP function globally in the device. The device participates in GVRP message exchanges. If the function is disabled, then the device ignores GVRP messages.

Possible values:

- **On**
  - The GVRP function is enabled.
- **Off** (default setting)
  - The GVRP function is disabled.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GVRP active</td>
<td>Activates/deactivates the port GVRP participation.</td>
</tr>
</tbody>
</table>

The prerequisite is that the GVRP function is globally enabled.

Possible values:

- **marked** (default setting)
  - The port GVRP participation is active.
- **unmarked**
  - The port GVRP participation is inactive.
5.7 **QoS/Priority**

Communication networks transmit a number of applications at the same time that have different requirements as regards availability, bandwidth and latency periods.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. You therefore have the possibility of providing minimum bandwidth for necessary applications. The prerequisite is that the end devices and the devices in the network support prioritized data transmission. Data packets with high priority are given preference when transmitted by devices in the network. You transfer data packets with lower priority when there are no data packets with a higher priority to be transmitted.

The device provides the following setting options:
- You specify how the device evaluates QoS/prioritization information for inbound data packets.
- For outbound packets, you specify which QoS/prioritization information the device writes in the data packet (for example priority for management packets, port priority).

**Note:** If you use the functions in this menu, then disable the flow control. The flow control is inactive if in the **Switching > Global** dialog, **Configuration** frame the **Flow control** checkbox is unmarked.

The menu contains the following dialogs:
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
- IP DSCP Mapping
- Queue Management
5.7.1 QoS/Priority Global

The device lets you maintain access to the device management, even in situations with heavy utilization. In this dialog you specify the required QoS/priority settings.

Configuration

VLAN priority for management packets

Specifies the VLAN priority for sending management data packets. Depending on the VLAN priority, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port.

Possible values:

- 0..7 (default setting: 0)

In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.

IP DSCP value for management packets

Specifies the IP DSCP value for sending management data packets. Depending on the IP DSCP value, the device assigns the data packet to a specific traffic class and thus to a specific priority queue of the port.

Possible values:

- 0 (be/cs0) .. 63 (default setting: 0 (be/cs0))

Some values in the list also have a DSCP keyword, for example 0 (be/cs0), 10 (af11) and 46 (ef). These values are compatible with the IP precedence model.

In the Switching > QoS/Priority > IP DSCP Mapping dialog you assign a traffic class to every IP DSCP value.

Queues per port

Displays the number of priority queues per port.

The device has 8 priority queues per port. You assign every priority queue to a specific traffic class (traffic class according to IEEE 802.1D).
5.7.2 QoS/Priority Port Configuration

In this dialog you specify for every port how the device processes received data packets based on their QoS/priority information.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>
| Port priority | Specifies what VLAN priority information the device writes into a data packet if the data packet contains no priority information. After this, the device transmits the data packet depending on the value specified in the Trust mode column. Possible values:
- 0..7 (default setting: 0) |
| Trust mode | Specifies how the device handles a received data packet if the data packet contains QoS/priority information. Possible values:
- untrusted
  - The device transmits the data packet according to the priority specified in the Port priority column. The device ignores the priority information contained in the data packet. In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.
- trustDot1p (default setting)
  - The device transmits the data packet according to the priority information in the VLAN tag. In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.
- trustIpDscp
  - If the data packet is an IP packet, then:
    - The device transmits the data packet according to the IP DSCP value contained in the data packet. In the Switching > QoS/Priority > IP DSCP Mapping dialog you assign a traffic class to every IP DSCP value.
  - If the data packet is not an IP packet, then:
    - The device transmits the data packet according to the priority specified in the Port priority column. In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.
Untrusted traffic class

Displays the traffic class assigned to the VLAN priority information specified in the Port priority column. In the Switching > QoS/Priority > 802.1D/p Mapping dialog, you assign a traffic class to every VLAN priority.

Possible values:

- 0..7
5.7.3 **802.1D/p Mapping**

The device transmits data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog you assign a *traffic class* to every VLAN priority. You assign the *traffic classes* to the priority queues of the ports.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>VLAN priority</th>
<th>Traffic class</th>
<th>Content description according to IEEE 802.1D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td><strong>Best Effort</strong> Normal data without prioritizing</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td><strong>Background</strong> Non-time-sensitive data and background services</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td><strong>Standard</strong> Normal data</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td><strong>Excellent Effort</strong> Crucial data</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td><strong>Controlled Load</strong> Time-sensitive data with a high priority</td>
</tr>
</tbody>
</table>

Note: Among other things redundancy mechanisms use the highest *traffic class*. Therefore, select another *traffic class* for application data.
<table>
<thead>
<tr>
<th>VLAN Priority</th>
<th>Traffic class</th>
<th>Content description according to IEEE 802.1D</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Video transmission with delays and jitter &lt; 100 ms</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Voice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voice transmission with delays and jitter &lt; 10 ms</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Network Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data for network management and redundancy mechanisms</td>
</tr>
</tbody>
</table>
5.7.4 **IP DSCP Mapping**

The device transmits IP data packets according to the DSCP value contained in the data packet with a higher or lower priority.

In this dialog you assign a *traffic class* to every DSCP value. You assign the *traffic classes* to the priority queues of the ports.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>DSCP Name</th>
<th>Traffic class</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort /CS0</td>
<td>2</td>
</tr>
<tr>
<td>1-7</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>CS1</td>
<td>0</td>
</tr>
<tr>
<td>9,11,13,15</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>10,12,14</td>
<td>AF11,AF12,AF13</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>CS2</td>
<td>1</td>
</tr>
<tr>
<td>17,19,21,23</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>18,20,22</td>
<td>AF21,AF22,AF23</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>CS3</td>
<td>3</td>
</tr>
<tr>
<td>25,27,29,31</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>26,28,30</td>
<td>AF31,AF32,AF33</td>
<td>3</td>
</tr>
<tr>
<td>32</td>
<td>CS4</td>
<td>4</td>
</tr>
<tr>
<td>33,35,37,39</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>34,36,38</td>
<td>AF41,AF42,AF43</td>
<td>4</td>
</tr>
<tr>
<td>40</td>
<td>CS5</td>
<td>5</td>
</tr>
<tr>
<td>41,42,43,44,45,47</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>DSCP Value</td>
<td>DSCP Name</td>
<td>Traffic class</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>46</td>
<td>EF</td>
<td>5</td>
</tr>
<tr>
<td>48</td>
<td>CS6</td>
<td>6</td>
</tr>
<tr>
<td>49-55</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>56</td>
<td>CS7</td>
<td>7</td>
</tr>
<tr>
<td>57-63</td>
<td></td>
<td>7</td>
</tr>
</tbody>
</table>
5.7.5 Queue Management

This dialog lets you enable and disable the Strict priority function for the traffic classes. When you disable the Strict priority function, the device processes the priority queues of the ports with Weighted Fair Queuing.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Traffic class</th>
<th>Displays the traffic class.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict priority</td>
<td>Activates/deactivates the processing of the port priority queue with Strict priority for this traffic class. Possible values:</td>
</tr>
<tr>
<td>marked</td>
<td>The processing of the port priority queue with Strict priority is active. The port forwards only data packets that are in the priority queue with the highest priority. When this priority queue is empty, the port forwards data packets that are in the priority queue with the next lower priority. The port forwards data packets with a lower traffic class after the priority queues with a higher priority are empty. In unfavorable situations, the port does not send these data packets. When you select this setting for a traffic class, the device also enables the function for traffic classes with a higher priority. Use this setting for applications such as VoIP or video that require the least possible delay.</td>
</tr>
<tr>
<td>unmarked</td>
<td>The processing of the port priority queue with Strict priority is inactive. The device uses Weighted Fair Queuing (WRR) to process the port priority queue. The device assigns a minimum bandwidth to each traffic class. Even under a high network load the port transmits data packets with a low traffic class. When you select this setting for a traffic class, the device also disables the function for traffic classes with a lower priority.</td>
</tr>
<tr>
<td>Min. bandwidth [%]</td>
<td>Specifies the minimum bandwidth for this traffic class when the device is processing the priority queues of the ports with Weighted Fair Queuing. Possible values:</td>
</tr>
</tbody>
</table>
| 0..100 | (default setting: 0 = the device does not reserve any bandwidth for this traffic class) The value specified in percent refers to the available bandwidth on the port. When you disable the Strict priority function for every traffic class, the maximum bandwidth is available on the port for the Weighted Fair Queuing. The maximum total of the assigned bandwidths is 100 %.
5.8 VLAN

With VLAN (Virtual Local Area Network) you distribute the data packets in the physical network to logical subnetworks. This provides you with the following advantages:

- **High flexibility**
  - With VLAN you distribute the data packets to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
  - With VLAN you specify network segments independently of the location of the individual end devices.

- **Improved throughput**
  - In VLANs data packets can be transferred by priority. When the priority is high, the device transfers the data of a VLAN preferentially, for example for time-sensitive applications such as VoIP phone calls.
  - When the data packets and Broadcasts are distributed in small network segments instead of in the entire network, the network load is considerably reduced.

- **Increased security**
  The distribution of the data packets among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based “tagged” VLANs according to the IEEE 802.1Q standard. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device transmits the tagged data packets of a VLAN only on ports that are assigned to the same VLAN. This reduces the network load.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

The device prioritizes the received data stream in the following sequence:
- Voice VLAN
- Port-based VLAN

The menu contains the following dialogs:
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice
5.8.1 VLAN Global

This dialog lets you view general VLAN parameters for the device.

Configuration

Buttons

🗑️ Reset VLAN settings

Resets the VLAN settings of the device to the default setting.

Note that you lose your connection to the device if you have changed the VLAN ID for the device management in the Basic Settings > Network > Global dialog.

Max. VLAN ID

Highest ID assignable to a VLAN.

See the Switching > VLAN > Configuration dialog.

VLANs (max.)

Displays the maximum number of VLANs possible.

See the Switching > VLAN > Configuration dialog.

VLANs

Number of VLANs currently configured in the device.

See the Switching > VLAN > Configuration dialog.

The VLAN ID 1 is constantly present in the device.
5.8.2 VLAN Configuration

In this dialog you manage the VLANs. To set up a VLAN, create a further table row. There you specify for each port if it transmits data packets of the respective VLAN and if the data packets contain a VLAN tag.

You distinguish between the following VLANs:
- The user sets up static VLANs.
- The device sets up dynamic VLANs automatically and removes them if the prerequisites cease to apply.
  For the following functions the device creates dynamic VLANs:
  - **MRP**: If you assign to the ring ports a non-existing VLAN, then the device creates this VLAN.
  - **MVRP**: The device creates a VLAN based on the messages of neighboring devices.

**Note**: The settings are effective only if the VLAN-unaware mode function is inactive. See the Switching > Global dialog.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  Opens the Create window to add a table row.
  In the **VLAN ID** field, you specify the ID of the VLAN.

- **Remove**
  Removes the selected table entry.

**VLAN ID**

ID of the VLAN.

The device supports up to 128 VLANs simultaneously set up.
Switching

[Switching > VLAN > Configuration]

Possible values:

- 1..4042

Status

Displays how the VLAN is set up.

Possible values:

- other
  - VLAN set up using the 802.1X function. See the Network Security > 802.1X dialog.
- permanent
  - VLAN set up by the user.
  - or
  - VLAN set up using the MRP function. See the Switching > L2-Redundancy > MRP dialog.
  - If you save the settings in the non-volatile memory, then the VLANs with this setting remain set up after a restart.
- dynamicMvrp
  - VLAN set up using the MVRP function. See the Switching > MRP-IEEE > MVRP dialog.
  - VLANs with this setting are write-protected. The device removes a VLAN from the table as soon as the last port leaves the VLAN.

Creation time

Displays the time of VLAN creation.

The field displays the time stamp for the operating time (system uptime).

Name

Specifies the name of the VLAN.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

<Port number>

Specifies if the respective port transmits data packets of the VLAN and if the data packets contain a VLAN tag.

Possible values:

- - (default setting)
  - The port is not a member of the VLAN and does not transmit data packets of the VLAN.
- T = Tagged
  - The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example.
- LT = Tagged Learned
  - The port is a member of the VLAN and transmits the data packets with a VLAN tag. The device created the entry automatically based on the GVRP or MVRP function.
- F = Forbidden
  - The port is not a member of the VLAN and does not transmit data packets of this VLAN. Additionally, the device helps prevent the port from becoming a VLAN member through the MVRP function.
Switching
[Switching > VLAN > Configuration]

- **U** = Untagged (default setting for VLAN 1)
  The port is a member of the VLAN and transmits the data packets without a VLAN tag. Use this setting if the connected device does not evaluate any VLAN tags, for example on end ports.

- **LU** = Untagged Learned
  The port is a member of the VLAN and transmits the data packets without a VLAN tag. The device created the entry automatically based on the GVRP or MVRP function.

**Note:** Verify that the port on which the network management station is connected is a member of the VLAN in which the device transmits the management data. In the default setting, the device transmits the management data on VLAN 1. Otherwise, the connection to the device terminates when you transfer the changes to the device. The access to the device management is possible only using the Command Line Interface through the serial interface.
5.8.3 VLAN Port

In this dialog you specify how the device handles received data packets that have no VLAN tag, or whose VLAN tag differs from the VLAN ID of the port.

This dialog lets you assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device transmits data packets if the VLAN-unaware mode function is inactive and one of the following situations occurs:

- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
- The VLAN tagging of the data packet differs from the VLAN ID of the port.

**Note:** The settings are effective only if the VLAN-unaware mode function is inactive. See the Switching > Global dialog.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

| Port-VLAN ID | Specifies the ID of the VLAN which the device assigns to data packets without a VLAN tag. |

Prerequisites:

- In the Acceptable packet types column the value admitAll is specified.

Possible values:

- 1..4042 (default setting: 1)
  - ID of a VLAN you set up.

If you use the MRP function and you did not assign a VLAN to the ring ports, then you specify the value 1 here for the ring ports. Otherwise, the device assigns the value to the ring ports automatically.

| Acceptable packet types | Specifies if the port transmits or discards received data packets without a VLAN tag. |

Possible values:

- admitAll (default setting)
  - The port accepts data packets both with and without a VLAN tag.
- admitOnlyVlanTagged
  - The port accepts only data packets tagged with a VLAN ID ≥ 1.
Ingress filtering

Activates/deactivates the ingress filtering.

Possible values:

- **marked**
  The ingress filtering is active.
  The device compares the VLAN ID in the data packet with the VLANs of which the device is a member. See the `Switching > VLAN > Configuration` dialog. If the VLAN ID in the data packet matches one of these VLANs, then the port transmits the data packet. Otherwise, the device discards the data packet.

- **unmarked** (default setting)
  The ingress filtering is inactive.
  The device transmits received data packets without comparing the VLAN ID. Thus the port also transmits data packets with a VLAN ID of which the port is not a member.
5.8.4 **VLAN Voice**

Use the Voice VLAN feature to separate voice and data packets on a port, by VLAN and/or priority. A primary benefit of Voice VLAN is safeguarding the quality of voice data when the port has a high load.

The device detects VoIP phones using the Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). The device then adds the appropriate port to the member set of the configured Voice VLAN. The member set is either tagged or untagged. Tagging depends on the Voice VLAN interface mode (VLAN ID, Dot1p, None, Untagged).

Another benefit of the Voice VLAN feature is that the VoIP phone obtains VLAN ID or priority information from the device using LLDP-MED. As a result, the VoIP phone sends voice data tagged as priority, or untagged. This depends on the configured Voice VLAN Interface mode. You activate Voice VLAN on the port which is connecting to the VoIP phone.

**Operation**

Enables/disables the Voice function of the device globally.

Possible values:
- **On**
- **Off** (default setting)

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
</table>

**Voice VLAN mode**

Specifies if the port transmits or discards received data packets without voice VLAN tagging or with voice VLAN priority information.

Possible values:
- **disabled** (default setting)
  - Deactivates the Voice function for this table row.
- **none**
  - Lets the IP telephone use its own configuration for sending untagged voice data packets.
- **vlan/dot1p-priority**
  - The port filters data packets of the voice VLAN using the vlan and dot1p priority tags.
- **untagged**
  - The port filters data packets without a voice VLAN tag.
Switching
[Switching > VLAN > Voice]

- **vlan**
  The port filters data packets of the voice VLAN using the vlan tag.

- **dot1p-priority**
  The port filters data packets of the voice VLAN using the dot1p priority tags. If you select this value, then additionally specify a proper value in the *Priority* column.

**Data priority mode**

Specifies the trust mode for the data packets on the particular port.

The device uses this mode for data packets on the voice VLAN, when it detects a VoIP telephone and a PC and when these devices use the same cable for transmitting and receiving data.

Possible values:

- **trust** (default setting)
  If voice data packets are present on the interface, then the data packets have the normal priority.

- **untrust**
  If voice data packets are present and the value *dot1p-priority* is specified in the *Voice VLAN mode* column, then the data packets have the priority 0. If the interface only transmits data, then the data has the normal priority.

**Status**

Displays the status of the Voice VLAN on the port.

Possible values:

- **marked**
  The Voice VLAN is enabled.

- **unmarked**
  The Voice VLAN is disabled.

**VLAN ID**

Specifies the ID of the VLAN to which the table row applies. To forward data packets to this VLAN ID using this filter, select in the *Voice VLAN mode* column the value *vlan*.

Possible values:

- **1..4042** (default setting: 1)

**Priority**

Specifies the Voice VLAN Priority of the port.

Prerequisites:

- In the *Voice VLAN mode* column the value *dot1p-priority* is specified.

Possible values:

- **0..7**
- **none**
  Deactivates the Voice VLAN Priority of the port.
DSCP

Specifies the IP DSCP value.

Possible values:

- 0 (be/cs0) to 63 (default setting: 0 (be/cs0))

Some values in the list also have a DSCP keyword, for example 0 (be/cs0), 10 (af11) and 46 (ef). These values are compatible with the IP precedence model.

In the Switching > QoS/Priority > IP DSCP Mapping dialog you assign a traffic class to every IP DSCP value.

Bypass authentication

Activates the Voice VLAN Authentication mode.

If you deactivate the function and set the value in the Voice VLAN mode column to dot1p-priority, then voice devices require an authentication.

Possible values:

- marked (default setting)
  - If you activated the function in the Network Security > 802.1X > Global dialog, then set the Port control parameter for this port to the multiClient value before activating this function. You find the Port control parameter in the Network Security > 802.1X > Global dialog.
- unmarked

5.9 L2-Redundancy

The menu contains the following dialogs:

- MRP
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet
5.9.1 MRP

The Media Redundancy Protocol (MRP) is a protocol that lets you set up high-availability, ring-shaped network structures. An MRP Ring with Hirschmann devices is made up of up to 100 devices that support the MRP protocol according to IEC 62439.

If a section is not operating, then the ring structure of an MRP Ring changes back into a line structure. The maximum recovery time can be configured.

The Ring Manager function of the device closes the ends of a backbone in a line structure to a redundant ring.

Note: Spanning Tree and Ring Redundancy have an effect on each other. Deactivate the Spanning Tree protocol for the ports connected to the MRP Ring. See the Switching > L2-Redundancy > Spanning Tree > Port dialog.

Operation

Buttons

Delete ring configuration
Disables the redundancy function and resets the settings in the dialog to the default setting.

Operation

Enables/disables the MRP function.
After you configured the parameters for the MRP Ring, enable the function here.

Possible values:

- **On**
  - The MRP function is enabled.
  - After you configured the devices in the MRP Ring, the redundancy is active.

- **Off** (default setting)
  - The MRP function is disabled.

Ring port 1/Ring port 2

Port

Specifies the number of the port that is operating as a ring port.

Possible values:

- `<Port number>`
  - Number of the ring port
Operation

Displays the operating status of the ring port.

Possible values:

- **forwarding**
  The port is enabled, connection exists.

- **blocked**
  The port is blocked, connection exists.

- **disabled**
  The port is disabled.

- **not-connected**
  No connection exists.

Fixed backup

Activates/deactivates the backup port function for the Ring port 2.

**Note:** The switch over to the primary port can exceed the maximum ring recovery time.

Possible values:

- **marked**
  The Ring port 2 backup function is active. When the ring is closed, the ring manager reverts back to the primary ring port.

- **unmarked** (default setting)
  The Ring port 2 backup function is inactive. When the ring is closed, the ring manager continues to send data on the secondary ring port.

Configuration

Ring manager

Enables/disables the Ring manager function.

If there is one device at each end of the line, then you activate this function.

Possible values:

- **On**
  The Ring manager function is enabled.
  The device operates as a ring manager.

- **Off** (default setting)
  The Ring manager function is disabled.
  The device operates as a ring client.
Advanced mode

Activates/deactivates the advanced mode for fast recovery times.

Possible values:
- **marked** (default setting)
  Advanced mode active.
  MRP-capable Hirschmann devices support this mode.
- **unmarked**
  Advanced mode inactive.
  Select this setting if another device in the ring does not support this mode.

Ring recovery

Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective if the device operates as a ring manager.

Possible values:
- 500ms
- 200ms (default setting)

Shorter switching times make greater demands on the response time of every individual device in the ring. Use values lower than 500ms if the other devices in the ring also support this shorter recovery time.

VLAN ID

Specifies the ID of the VLAN which you assign to the ring ports.

Possible values:
- 0 (default setting)
  No VLAN assigned.
  Assign in the **Switching > VLAN > Configuration** dialog to the ring ports for VLAN 1 the value U.
- 1..4042
  VLAN assigned.
  If you assign to the ring ports a non-existing VLAN, then the device creates this VLAN. In the **Switching > VLAN > Configuration** dialog, the device creates a table row for the VLAN and assigns the value T to the ring ports.

Information

Displays messages for the redundancy configuration and the possible causes of detected errors.

When the device operates as a ring client or a ring manager, the following messages are possible:
- **Redundancy available**
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- **Configuration error: Error on ringport link.**
  An error is detected in the cabling of the ring ports.
When the device operates as a ring manager, the following messages are possible:

- Configuration error: Packets from another ring manager received.  
  Another device exists in the ring that operates as the ring manager.  
  Enable the Ring manager function only on one device in the ring.

- Configuration error: Ring link is connected to wrong port.  
  A line in the ring is connected with a different port instead of with a ring port.  
  The device only receives test data packets on one ring port.

### 5.9.2 Spanning Tree

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network in order to help avoid loops. If a network component becomes inoperative on the path, then the device calculates the new topology and reactivates these paths.

The Rapid Spanning Tree Protocol (RSTP) enables fast switching to a newly calculated topology without interrupting existing connections. RSTP gets average reconfiguration times of less than a second. When you use RSTP in a ring with 10 to 20 devices, you can get reconfiguration times in the order of milliseconds.

Note: When you connect the device to the network through twisted pair SFPs instead of through usual twisted pair ports, the reconfiguration of the network takes slightly longer.

The menu contains the following dialogs:

- Spanning Tree Global
- Spanning Tree Port
5.9.2.1 Spanning Tree Global

In this dialog you enable/disable the Spanning Tree function and specify the bridge settings.

Operation

Enables/disables the Spanning Tree function in the device.

Possible values:

- **On** (default setting)
- **Off**
  
  The device behaves transparently. The device floods received Spanning Tree data packets like multicast data packets to the ports.

Variant

Displays the protocol used for the Spanning Tree function:

Possible values:

- **rstp**
  
  The protocol RSTP is active.
  
  With RSTP (IEEE 802.1Q-2005), the Spanning Tree function operates for the underlying physical layer.

Traps

Activates/deactivates the sending of SNMP traps for the following events:

- Another bridge takes over the root bridge role.
- The topology changes. A port changes its Port state from forwarding into discarding or from discarding into forwarding.

Possible values:

- **marked** (default setting)
  
  The sending of SNMP traps is active.
- **unmarked**
  
  The sending of SNMP traps is inactive.
**Bridge configuration**

**Bridge ID**

Displays the bridge ID of the device.

The device with the lowest bridge ID numerical value takes over the role of the root bridge in the network.

Possible values:
- `<Bridge priority> / <MAC address>`
  - Value in the *Priority* field / MAC address of the device

**Priority**

Specifies the bridge priority of the device.

Possible values:
- `0..61440` in steps of 4096 (default setting: `32768`)

To make this device the root bridge, assign the lowest numeric priority value in the network to the device.

**Hello time [s]**

Specifies the time in seconds between the sending of two configuration messages (Hello data packets).

Possible values:
- `1..2` (default setting: `2`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

Due to the interaction with the *Tx holds* parameter, we recommend that you do not change the default setting.

**Forward delay [s]**

Specifies the delay time for the status change in seconds.

Possible values:
- `4..30` (default setting: `15`)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The *Spanning Tree* protocol uses the parameter to delay the status change between the statuses `disabled, discarding, learning, forwarding`.

The parameters *Forward delay [s]* and *Max age* have the following relationship:
**Forward delay [s] ≥ (Max age/2) + 1**

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

### Max age

Specifies the maximum permitted branch length for example, the number of devices to the root bridge.

Possible values:
- 6..40 (default setting: 20)

If the device takes over the role of the root bridge, then the other devices in the network use the value specified here.

Otherwise, the device uses the value specified by the root bridge. See the *Root information* frame.

The *Spanning Tree* protocol uses the parameter to specify the validity of STP-BPDUs in seconds.

### Tx holds

Limits the maximum transmission rate for sending BPDUs.

Possible values:
- 1..40 (default setting: 10)

When the device sends a BPDU, the device increments a counter on this port.

If the counter reaches the value specified here, then the port stops sending BPDUs. On the one hand, this reduces the load generated by RSTP, and on the other when the device does not receive BPDUs, a communication interruption can be caused.

The device decrements the counter by 1 every second. In the following second, the device sends a maximum of 1 new BPDU.

### BPDU guard

Activates/deactivates the BPDU Guard function in the device.

With this function, the device helps protect your network from incorrect configurations, attacks with STP-BPDUs, and unwanted topology changes.

Possible values:
- **marked**
  - The *BPDU guard* is active.
  - The device applies the function to manually specified edge ports. For these ports, in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab the checkbox in the *Admin edge port* column is marked.
  - If an edge port receives an STP-BPDU, then the device disables the port. For this port, in the *Basic Settings > Port* dialog, *Configuration* tab the checkbox in the *Port on* column is unmarked.
- **unmarked** (default setting)
  - The *BPDU guard* is inactive.
To reset the status of the port to the value *forwarding*, you proceed as follows:

- If the port is still receiving BPDUs, then:
  - In the Switching > L2-Redundancy > Spanning Tree > Port dialog, CIST tab unmark the checkbox in the Admin edge port column.
  - or
  - In the Switching > L2-Redundancy > Spanning Tree > Global dialog, unmark the BPDU guard checkbox.

- To re-enable the port again you use the Auto-Disable function. Alternatively, proceed as follows:
  - Open the Basic Settings > Port dialog, Configuration tab.
  - Mark the checkbox in the Port on column.

**BPDU filter (all admin edge ports)**

Activates/deactivates the STP-BPDU filter on every manually specified edge port. For these ports, in the Switching > L2-Redundancy > Spanning Tree > Port dialog, CIST tab the checkbox in the Admin edge port column is marked.

Possible values:

- **marked**
  - The BPDU filter is active on every edge port.
  - The function does not use these ports in Spanning Tree operations.
  - The device does not send STP-BPDUs on these ports.
  - The device drops any STP-BPDUs received on these ports.

- **unmarked** (default setting)
  - The global BPDU filter is inactive.
  - You have the option to explicitly activate the BPDU filter for single ports. See the Port BPDU filter column in the Switching > L2-Redundancy > Spanning Tree > Port dialog.

**Auto-disable**

Activates/deactivates the Auto-Disable function for the parameters that BPDU guard is monitoring on the port.

Possible values:

- **marked**
  - The Auto-Disable function for the BPDU guard is active.
  - When the port receives an STP-BPDU, the device disables an edge port. The Link status LED for the port flashes 3× per period.
  - The Diagnostics > Ports > Auto-Disable dialog displays which ports are currently disabled due to the parameters being exceeded.
  - After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the Diagnostics > Ports > Auto-Disable dialog and specify a waiting period for the relevant port in the Reset timer [s] column.

- **unmarked** (default setting)
  - The Auto-Disable function for the BPDU guard is inactive.
Root information

Root ID
Displays the bridge ID of the current root bridge.

Possible values:
▶ <Bridge priority> / <MAC address>

Priority
Displays the bridge priority of the current root bridge.

Possible values:
▶ 0..61440 in steps of 4096

Hello time [s]
Displays the time in seconds that the root bridge specifies between the sending of two configuration messages (Hello data packets).

Possible values:
▶ 1..2

The device uses this specified value. See the Bridge configuration frame.

Forward delay [s]
Displays the delay time in seconds set up by the root bridge for status changes.

Possible values:
▶ 4..30

The device uses this specified value. See the Bridge configuration frame.

In the RSTP protocol, the bridges negotiate a status change without a specified delay.

The Spanning Tree protocol uses the parameter to delay the status change between the statuses disabled, discarding, learning, forwarding.

Max age
Specifies the maximum permitted branch length that the root bridge sets up for example, the number of devices to the root bridge.

Possible values:
▶ 6..40 (default setting: 20)

The Spanning Tree protocol uses the parameter to specify the validity of STP-BPDUs in seconds.
**Topology information**

**Bridge is root**

Displays if the device currently has the role of the root bridge.

Possible values:
- **marked**
  - The device currently has the role of the root bridge.
- **unmarked**
  - Another device currently has the role of the root bridge.

**Root port**

Displays the number of the port from which the current path leads to the root bridge.

If the device takes over the role of the root bridge, then the field displays the value `no Port`.

**Root path cost**

Displays the path cost for the path that leads from the root port of the device to the root bridge of the layer 2 network.

Possible values:
- **0**
  - The device takes over the role of the root bridge.
- **1..200000000**

**Topology changes**

Displays how many times the device has put a port into the forwarding status using the Spanning Tree function since the Spanning Tree instance was started.

**Time since topology change**

Displays the time since the last topology change.

Possible values:
- `<days, hours:minutes:seconds>`
5.9.2.2 Spanning Tree Port

In this dialog you activate the Spanning Tree function on the ports, specify edge ports, and specify the settings for various protection functions.

The dialog contains the following tabs:
- [CIST]
- [Guards]

[CIST]

In this tab you have the option to activate the Spanning Tree function on the ports individually, specify the settings for edge ports, and view the current values. The abbreviation CIST stands for Common and Internal Spanning Tree.

Note: Deactivate the Spanning Tree function on the ports that are participating in other Layer 2 redundancy protocols. Otherwise, it is possible that the redundancy protocols operate differently than intended. This can cause loops.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP active</td>
<td>Activates/deactivates the Spanning Tree function on the port.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>marked (default setting)</td>
<td>The Spanning Tree function is active on the port.</td>
</tr>
<tr>
<td>unmarked</td>
<td>The Spanning Tree function is inactive on the port. If the Spanning Tree function is enabled in the device and inactive on the port, then the port does not send STP-BPDUs and drops any STP-BPDUs received.</td>
</tr>
<tr>
<td>Port state</td>
<td>Displays the transmission status of the port.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
<tr>
<td>discarding</td>
<td>The port is blocked and forwards only STP-BPDUs.</td>
</tr>
<tr>
<td>learning</td>
<td>The port is blocked, but it learns the MAC addresses of received data packets.</td>
</tr>
</tbody>
</table>
- **forwarding**
  The port forwards data packets.

- **disabled**
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

- **manualFwd**
  The *Spanning Tree* function is disabled on the port. The port forwards STP-BPDUs.

- **notParticipate**
  The port is not participating in STP.

### Port role

Displays the current role of the port in the CIST.

**Possible values:**

- **root**
  Port with the cheapest path to the root bridge.

- **alternate**
  Port with the alternative path to the root bridge (currently blocking).

- **designated**
  Port for the side of the tree averted from the root bridge (currently blocking).

- **backup**
  Port receives STP-BPDUs from its own device.

- **disabled**
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

### Port path cost

Specifies the path costs of the port.

**Possible values:**

- **0..200000000** (default setting: 0)

  When the value is 0, the device automatically calculates the path costs depending on the data rate of the port.

### Port priority

Specifies the priority of the port.

**Possible values:**

- **16..240** in steps of 16  (default setting: 128)

  This value represents the first 4 bits of the port ID.
Received bridge ID

Displays the bridge ID of the device from which this port last received an STP-BPDU.

Possible values:

- For ports with the designated role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the alternate, backup, master, and root port roles, in the stationary condition (static topology) this information is identical to the information of the designated port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the designated role.

Received port ID

Displays the port ID of the device from which this port last received an STP-BPDU.

Possible values:

- For ports with the designated role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the alternate, backup, master, and root port roles, in the stationary condition (static topology) this information is identical to the information of the designated port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the designated role.

Received path cost

Displays the path cost that the higher-level bridge has from its root port to the root bridge.

Possible values:

- For ports with the designated role, the device displays the information for the STP-BPDU last received by the port. This helps to diagnose the possible STP problems in the network.
- For the alternate, backup, master, and root port roles, in the stationary condition (static topology) this information is identical to the information of the designated port role.
- If a port has no connection or if it did not receive any STP-BDPUs yet, then the device displays the values that the port can send with the designated role.

Admin edge port

Activates/deactivates the Admin edge port mode. If the port is connected to an end device, then use the Admin edge port mode. This setting lets the edge port change faster to the forwarding state after linkup and thus a faster accessibility of the end device.

Possible values:

- marked
  The Admin edge port mode is active. The port is connected to an end device.
  - After the connection is set up, the port changes to the forwarding status without changing to the learning status beforehand.
  - If the port receives an STP-BPDU and the BPDU Guard function is active, then the device deactivates the port. See the Switching > L2-Redundancy > Spanning Tree > Global dialog.
- unmarked (default setting)
  The Admin edge port mode is inactive. The port is connected to another STP bridge. After the connection is set up, the port changes to the learning status before changing to the forwarding status, if applicable.
Auto edge port

Activates/deactivates the automatic detection of whether you connect an end device to the port. The prerequisite is that the checkbox in the Admin edge port column is unmarked.

Possible values:
- **marked** (default setting)
  - The automatic detection is active.
  - After the installation of the connection and after $1.5 \times \text{Hello time [s]}$, the device sets the port to the forwarding status. (default setting $1.5 \times 2 \text{ s}$) if the port did not receive any STP-BPDUs during this time.
- **unmarked**
  - The automatic detection is inactive.
  - After the installation of the connection, and after Max age the device sets the port to the forwarding status.
  - (default setting: 20 s)

Oper edge port

Displays if an end device or an STP bridge is connected to the port.

Possible values:
- **marked**
  - An end device is connected to the port. The port does not receive any STP-BPDUs.
- **unmarked**
  - An STP bridge is connected to the port. The port receives STP-BPDUs.

Oper PointToPoint

Displays if the port is connected to an STP device through a direct full-duplex link.

Possible values:
- **marked**
  - The port is connected directly to an STP device through a full-duplex link. The direct, decentralized communication between 2 bridges provides short reconfiguration times.
- **unmarked**
  - The port is connected in another way, for example through a half-duplex link or through a hub.

Port BPDU filter

Activates/deactivates the filtering of STP-BPDUs on the port explicitly.

The prerequisite is that the port is a manually specified edge port. For these ports, the checkbox in the Admin edge port column is marked.

Possible values:
- **marked**
  - The BPDU filter is active on the port.
  - The function excludes the port from Spanning Tree operations.
    - The device does not send STP-BPDUs on the port.
    - The device drops any STP-BPDUs received on the port.
- **unmarked** (default setting)
  - The BPDU filter is inactive on the port.

You have the option to globally activate the BPDU filter for every edge port. See the Switching > L2-Redundancy > Spanning Tree > Global dialog, Bridge configuration frame. If the BPDU filter (all admin edge ports) checkbox is marked, then the BPDU filter is still active on the port.
BPDU filter status

Displays if the BPDU filter is active on the port.

Possible values:

- **marked**
  - The BPDU filter is active on the port as a result of the following settings:
    - The checkbox in the Port BPDU filter column is marked.
    - or
    - The checkbox in the BPDU filter (all admin edge ports) column is marked. See the Switching > L2-Redundancy > Spanning Tree > Global dialog, Bridge configuration frame.

- **unmarked**
  - The BPDU filter is inactive on the port.

BPDU flood

Activates/deactivates the BPDU flood mode on the port even if the Spanning Tree function is inactive on the port. The device floods STP-BPDUs received on the port to the ports for which the Spanning Tree function is inactive and the BPDU flood mode is active too.

Possible values:

- **marked**
  - The BPDU flood mode is active.

- **unmarked** (default setting)
  - The BPDU flood mode is inactive.

[Guards]

This tab lets you specify the settings for various protection functions on the ports.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Port**

Displays the port number.

**Root guard**

Activates/deactivates the monitoring of STP-BPDUs on the port. The prerequisite is that the Loop guard function is inactive.

With this setting the device helps you protect your network from incorrect configurations or attacks with STP-BPDUs that try to change the topology. This setting is relevant only for ports with the STP role designated.
Possible values:

- **marked**
  The monitoring of STP-BPDUs is active.
  - If the port receives an STP-BPDU with better path information to the root bridge, then the device discards the STP-BPDU and sets the status of the port to the value `discarding` instead of `root`.
  - If there are no STP-BPDUs with better path information to the root bridge, then the device resets the status of the port after `2 × Hello time [s]`.

- **unmarked** (default setting)
  The monitoring of STP-BPDUs is inactive.

**TCN guard**

Activates/deactivates the monitoring of "Topology Change Notifications" on the port. With this setting the device helps you protect your network from attacks with STP-BPDUs that try to change the topology.

Possible values:

- **marked**
  The monitoring of "Topology Change Notifications" is enabled.
  - The port ignores the Topology Change flag in received STP-BPDUs.
  - If the received BPDU contains other information that causes a topology change, then the device processes the BPDU even if the TCN guard is enabled.
    
    Example: The device receives better path information for the root bridge.

- **unmarked** (default setting)
  The monitoring of "Topology Change Notifications" is disabled.
  If the device receives STP-BPDUs with a Topology Change flag, then the device deletes the address table of the port and forwards the Topology Change Notifications.

**Loop guard**

Activates/deactivates the monitoring of loops on the port. The prerequisite is that the `Root guard` function is inactive.

With this setting the device helps prevent loops if the port does not receive any more STP-BPDUs. Use this setting only for ports with the STP role `alternate`, `backup` or `root`.

Possible values:

- **marked**
  The monitoring of loops is active. This helps prevent loops for example, if you disable the Spanning Tree function on the remote device or if the connection is interrupted only in the receiving direction.
  - If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value `discarding` and marks the checkbox in the `Loop state` column.
  - If the port receives STP-BPDUs again, then the device sets the status of the port to a value according to `Port role` and unmarks the checkbox in the `Loop state` column.

- **unmarked** (default setting)
  The monitoring of loops is inactive.
  If the port does not receive any STP-BPDUs for a while, then the device sets the status of the port to the value `forwarding`. 
Loop state

Displays if the loop state of the port is inconsistent.

Possible values:

- **marked**
  - The loop state of the port is inconsistent:
    - The port is not receiving any STP-BPDUs and the Loop guard function is enabled.
    - The device sets the state of the port to the value discarding. The device thus helps prevent any potential loops.

- **unmarked**
  - The loop state of the port is consistent. The port receives STP-BPDUs.

Trans. into loop

Displays how many times the loop state of the port became inconsistent (marked checkbox in the Loop state column).

Trans. out of loop

Displays how many times the loop state of the port became consistent (unmarked checkbox in the Loop state column).

BPDU guard effect

Displays if the port received an STP-BPDU as an edge port.

Prerequisite:

- The port is a manually specified edge port. In the Switching > L2-Redundancy > Spanning Tree > Port dialog, the checkbox for this port in the Admin edge port column is marked.
- In the Switching > L2-Redundancy > Spanning Tree > Global dialog, the BPDU Guard function is active.

Possible values:

- **marked**
  - The port is an edge port and received an STP-BPDU.
  - The device deactivates the port. For this port, in the Basic Settings > Port dialog, Configuration tab the checkbox in the Port on column is unmarked.

- **unmarked**
  - The port is an edge port and has not received any STP-BPDUs, or the port is not an edge port.

To reset the status of the port to the value forwarding, you proceed as follows:

- If the port is still receiving BPDUs, then:
  - In the CIST tab, unmark the checkbox in the Admin edge port column.
  - Or
  - In the Switching > L2-Redundancy > Spanning Tree > Global dialog, unmark the BPDU guard checkbox.

- To activate the port, proceed as follows:
  - Open the Basic Settings > Port dialog, Configuration tab.
  - Mark the checkbox in the Port on column.
5.9.3 **Link Aggregation**

The *Link Aggregation* function lets you aggregate multiple parallel links. The prerequisite is that the links have the same speed and are full duplex. The advantages compared to conventional connections using a single line are higher availability and a higher transmission bandwidth.

The Link Aggregation Control Protocol (LACP) makes it possible to monitor the packet-based continuous link status on the physical ports. LACP also helps ensure that the link partners meet the aggregation prerequisites.

If the remote side does not support the Link Aggregation Control Protocol (LACP), then you can use the *Static link aggregation* function. In this case, the device aggregates the links based on the link, link speed and duplex setting.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

**Add**

Opens the Create window to add a table row for a LAG interface or to assign a physical port to a LAG interface.

- From the Trunk port drop-down list, you select the LAG interface number.
- From the Port drop-down list, you select the number of a physical port to assign to the LAG interface.

After you create a LAG interface, the device adds the LAG interface to the table in the Basic Settings > Port dialog, Statistics tab.

**Remove**

Removes the selected table row.
Trunk port

Displays the LAG interface number.

Name

Specifies the name of the LAG interface.

Possible values:

- Alphanumeric ASCII character string with 1..15 characters

Link/Status

Displays the current operating state of the LAG interface and the physical ports.

Possible values:

- **up (lag/row)**
  - The LAG interface is operational.
  - The prerequisites are:
    - The *Static link aggregation* function is active on this LAG interface.
    - or
    - LACP is active on the physical ports assigned to the LAG interface, see the *LACP active* column.
    - and
    - The key specified for the LAG interface in the *LACP admin key* column matches the keys specified for the physical ports in the *LACP port actor admin key* column.
    - and
    - The number of operational physical ports assigned to the LAG interface is greater than or equal to the value specified in the *Active ports (min.)* column.

- **up**
  - The physical port is operational.

- **down (lag/row)**
  - The LAG interface is down.

- **down**
  - The physical port is disabled.
  - or
  - No cable connected or no active link.

Active

Activates/deactivates the LAG interface.

Possible values:

- **marked** (default setting)
  - The LAG interface is active.

- **unmarked**
  - The LAG interface is inactive.

STP active

Activates/deactivates the *Spanning Tree* protocol on this LAG interface. The prerequisite is that in the *Switching > L2-Redundancy > Spanning Tree > Global* dialog the *Spanning Tree* function is enabled.

You can also activate/deactivate the *Spanning Tree* protocol on the LAG interfaces in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
Possible values:
- **marked** (default setting)
  - The *Spanning Tree* protocol is active on this LAG interface.
- **unmarked**
  - The *Spanning Tree* protocol is inactive on this LAG interface.

**Static link aggregation**

Activates/deactivates the *Static link aggregation* function on the LAG interface. The device aggregates the assigned physical ports to the LAG interface, even if the remote site does not support LACP.

Possible values:
- **marked**
  - The *Static link aggregation* function is active on this LAG interface. The device aggregates an assigned physical port to the LAG interface as soon as the physical port gets a link. The device does not send LACPDUs and discards received LACPDUs.
- **unmarked** (default setting)
  - The *Static link aggregation* function is inactive on this LAG interface. If the connection was successfully negotiated using LACP, then the device aggregates an assigned physical port to the LAG interface.

**Active ports (min.)**

Specifies the minimum number of physical ports to be active for the LAG interface to stay active. If the number of active physical ports is lower than the specified value, then the device deactivates the LAG interface.

If a redundancy function like *Spanning Tree* or *MRP* over LAG is active in the device, then you use this function to force the device to switch automatically to the redundant line.

Possible values:
- **1** (default setting)
- **2**
- Depending on the hardware:
  - **4**
  - **8**
  - **32**

**Type**

Displays if the LAG interface is based on the *Static link aggregation* function or on LACP.

Possible values:
- **static**
  - The LAG interface is based on the *Static link aggregation* function.
- **dynamic**
  - The LAG interface is based on LACP.
Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status for this interface.

Possible values:
- **marked** (default setting)  
  The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.  
  If the device detects a link up/down status change, then the device sends an SNMP trap.
- **unmarked**  
  The sending of SNMP traps is inactive.

LACP admin key

Specifies the LAG interface key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:
- **0..65535**  
  You specify the corresponding value for the physical ports in the LACP port actor admin key column.

Port

Displays the physical port number assigned to the LAG interface.

Aggregation port status

Displays if the LAG interface aggregates the physical port.

Possible values:
- **active**  
  The LAG interface aggregates the physical port.
- **inactive**  
  The LAG interface does not aggregate the physical port.

LACP active

Activates/deactivates LACP on the physical port.

Possible values:
- **marked** (default setting)  
  LACP is active on the physical port.
- **unmarked**  
  LACP is inactive on the physical port.
LACP port actor admin key

Specifies the physical port key. The device uses this key to identify the ports that can be aggregated to the LAG interface.

Possible values:

- 0
  - The device ignores the key on this physical port when deciding to aggregate the port into the LAG interface.

- `1..65535`
  - If this value matches the value of the LAG interface specified in the LACP admin key column, then the device only aggregates this physical port to the LAG interface.

LACP actor admin state

Specifies the actor state values that the LAG interface transmits in the LACPDUs. This lets you control the LACPDUs parameters.

The device lets you mix the values. From the drop-down list, select one or more values.

Possible values:

- `ACT`
  - (LACP Activity state)
    - When selected, the link transmits the LACPDUs cyclically, otherwise when requested.

- `STO`
  - (LACP Timeout state)
    - When selected, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout.

- `AGG`
  - (Aggregation state)
    - When selected, the device interprets the link as a candidate for aggregation, otherwise as an individual link.

For further information on the values, see the standard IEEE 802.1AX-2014.

LACP actor oper state

Displays the actor state values that the LAG interface transmits in the LACPDUs.

Possible values:

- `ACT`
  - (LACP Activity state)
    - When visible, the link transmits the LACPDUs cyclically, otherwise when requested.

- `STO`
  - (LACP Timeout state)
    - When visible, the link transmits the LACPDUs cyclically using the short timeout, otherwise using the long timeout.

- `AGG`
  - (Aggregation state)
    - When visible, the device interprets the link as a candidate for aggregation, otherwise as an individual link.

- `SYN`
  - (Synchronization state)
    - When visible, the device interprets the link as IN_SYNC, otherwise as OUT_OF_SYNC.
COL
(Collecting state)
When visible, collection of incoming frames is enabled on this link, otherwise disabled.

DST
(Distributing state)
When visible, distribution of outgoing frames is enabled on this link, otherwise disabled.

DFT
(Defaulted state)
When visible, the link uses defaulted operational information, administratively specified for the Partner. Otherwise the link uses the operational information received from a LACPDU.

EXP
(Expired state)
When visible, the link receiver is in the EXPIRED state.

LACP partner oper SysID
Displays the MAC address of the remote device connected to this physical port.
The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port
Displays the port number of the remote device connected to this physical port.
The LAG interface has received this information in a LACPDU from the partner.

LACP partner oper port state
Displays the partner state values that the LAG interface receives in the LACPDU.
Possible values:
- ACT
- STO
- AGG
- SYN
- COL
- DST
- DFT
- EXP

For further information on the values, see the description of the LACP actor oper state column and the standard IEEE 802.1AX-2014.
5.9.4 **Link Backup**

With Link Backup, you configure pairs of redundant links. Each pair has a primary port and a backup port. The primary port forwards the data packets until the device detects an error. If the device detects an error on the primary port, then the Link Backup function transfers the data packets over to the backup port.

The dialog also lets you set a fail back option. If you enable the fail back function and the primary port returns to normal operation, then the device first blocks the data packets on the backup port and then forwards the data packets on the primary port. This process helps protect the device from causing loops in the network.

**Operation**

Enables/disables the Link Backup function globally in the device.

Possible values:

- **On** (default setting)
  
  Enables the Link Backup function.

- **Off**
  
  Disables the Link Backup function.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  
  Adds a table row.

- **Remove**
  
  Removes the selected table row.
Primary port

Displays the primary port of the interface pair. When you enable the Link Backup function, this port is responsible for forwarding the data packets.

Possible values:
- Physical ports

Backup port

Displays the backup port on which the device forwards the data packets if the device detects an error on the primary port.

Possible values:
- Physical ports except for the port you set as the primary port.

Description

Specifies the Link Backup pair. Enter a name to identify the Backup pair.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

Primary port status

Displays the status of the primary port for this Link Backup pair.

Possible values:
- **forwarding**
  - The link is up, no shutdown, and forwarding data packets.
- **blocking**
  - The link is up, no shutdown, and blocking data packets.
- **down**
  - The port is either link down, cable unplugged, or disabled in software, shutdown.
- **unknown**
  - The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.

Backup port status

Displays the status of the Backup port for this Link Backup pair.

Possible values:
- **forwarding**
  - The link is up, no shutdown, and forwarding data packets.
- **blocking**
  - The link is up, no shutdown, and blocking data packets.
- **down**
  - The port is either link down, cable unplugged, or disabled in the software, shutdown.
- **unknown**
  - The Link Backup feature is globally disabled, or the port pair is inactive. Therefore, the device ignores the port pair settings.
Fail back

Activates/deactivates the automatic fail back.

Possible values:

▶ **marked** (default setting)
  The automatic fail back is active. After the delay timer expires, the backup port changes to **blocking** and the primary port changes to **forwarding**.

▶ **unmarked**
  The automatic fail back is inactive. The backup port continues forwarding data packets even after the primary port re-establishes a link or you manually change the admin status of the primary port from **shutdown** to **no shutdown**.

Fail back delay [s]

Specifies the delay time in seconds that the device waits after the primary port re-establishes a link. Furthermore, this timer also applies when you manually set the admin status of the primary port from **shutdown** to **no shutdown**. After the delay timer expires, the backup port changes to **blocking** and the primary port changes to **forwarding**.

Possible values:

▶ **0..3600** (default setting: 30)
  When set to 0, immediately after the primary port re-establishes a link, the backup port changes to **blocking** and the primary port changes to **forwarding**. Furthermore, immediately after you manually set the admin status of from **shutdown** to **no shutdown**, the backup port changes to **blocking** and the primary port changes to **forwarding**.

Active

Activates/deactivates the Link Back up pair configuration.

Possible values:

▶ **marked**
  The Link Backup pair is active. The device senses the link and administration status and forwards the data packets according to the pair configuration.

▶ **unmarked** (default setting)
  The Link Backup pair is inactive. The ports forward the data packets according to standard switching.
Create

Primary port

Specifies the primary port of the backup interface pair. During normal operation this port is responsible for forwarding the data packets.

Possible values:
▶ Physical ports

Backup port

Specifies the backup port to which the device transfers the data packets to if the device detects an error on the primary port.

Possible values:
▶ Physical ports except for the port you set as the primary port.

5.9.5 FuseNet

The FuseNet protocols let you couple rings that are operating with one of the following redundancy protocols:
▶ MRP
▶ RSTP

The menu contains the following dialogs:
▶ Sub Ring
5.9.5.1 Sub Ring

This dialog lets you set up the device as a Sub Ring manager.

The **Sub Ring** function lets you easily couple network segments to existing redundancy rings. The Sub Ring manager (SRM) couples a Sub Ring to an existing ring (base ring).

In the Sub Ring you can use any devices that support MRP as ring participants. These devices do not require a Sub Ring manager function.

When setting up Sub Rings, remember the following rules:
- The device supports **Link Aggregation** in the Sub Ring
- No spanning tree on Sub Ring ports
- **Same MRP domain** on devices within a Sub Ring
- Different VLANs for base ring and Sub Ring

Specify the VLAN settings as follows:
- **VLAN x** for base ring
  - on the ring ports of the base ring participants
  - on the base ring ports of the Sub Ring manager
- **VLAN y** for Sub Ring
  - on the ring ports of the Sub Ring participants
  - on the Sub Ring ports of the Sub Ring manager

**Note:** To help avoid loops, only close the redundant line when the settings are specified in every device participating in the ring.

**Operation**

Enables/disables the **Sub Ring** function.

Possible values:
- **On**
  - The **Sub Ring** function is enabled.
- **Off** (default setting)
  - The **Sub Ring** function is disabled.

**Information**

Table entries (max.)

Displays the maximum number of Sub Rings supported by the device.
### Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

#### Buttons

- **Add**
  
  Adds a table row.

- **Remove**
  
  Removes the selected table row.

#### Sub Ring ID

Displays the unique identifier of this Sub Ring.

Possible values:

- 1..8

#### Name

Specifies the optional name of the Sub Ring.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

#### Active

Activates/deactivates the Sub Ring.

Activate the Sub Ring when the configuration of every Sub Ring device is complete. Close the Sub Ring only after activating the Sub Ring function.

Possible values:

- **marked**
  
  The Sub Ring is active.

- **unmarked** (default setting)
  
  The Sub Ring is inactive.

#### Configuration status

Displays the operational state of the Sub Ring configuration.

Possible values:

- **noError**
  
  The device detects an acceptable Sub Ring configuration.

- **ringPortLinkError**
  
  - The ring port has no link.
  
  - One of the Sub Ring lines is connected to one more port of the device. But the Sub Ring line is not connected to one of the ring ports of the device.
multipleSRM
The Sub Ring manager receives packets from more than one Sub Ring manager in the Sub Ring.

noPartnerManager
The Sub Ring manager receives its own frames.

concurrentVLAN
The MRP protocol in the base ring uses the VLAN of the Sub Ring manager domain.

concurrentPort
One more redundancy protocol uses the ring port of the Sub Ring manager domain.

concurrentRedundancy
The Sub Ring manager domain is inactive because of one more active redundancy protocol.

trunkMember
The ring port of the Sub Ring manager domain is member of a Link Aggregation connection.

sharedVLAN
The Sub Ring manager domain is inactive because shared VLAN is active and the main ring also uses the MRP protocol.

Redundancy available
Displays the operational state of the ring redundancy in the Sub Ring.

Possible values:
- redGuaranteed
  Redundancy reserve is available.
- redNotGuaranteed
  Loss of redundancy reserve.

Port
Specifies the port that connects the device to the Sub Ring.

Possible values:
- <Port number>

SRM mode
Specifies the mode of the Sub Ring manager.

A Sub Ring has 2 managers simultaneously that couple the Sub Ring to the base ring. As long as the Sub Ring is physically closed, one manager blocks its Sub Ring port.

Possible values:
- manager (default setting)
  The Sub Ring port forwards data packets.
  When this value is set on both devices that couple the Sub Ring to the base ring, the device with the higher MAC address functions as the redundantManager.
Switching
[Switching > L2-Redundancy > FuseNet > Sub Ring]

- **redundantManager**
  The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets. When this value is set on both devices that couple the Sub Ring to the base ring, the device with the higher MAC address functions as the redundantManager.

- **singleManager**
  Use this value when the Sub Ring is coupled to the base ring through one single device. The prerequisite is that there are 2 instances of the Sub Ring in the table. Assign this value to both instances. The Sub Ring port of the instance with the higher port number is blocked while the Sub Ring is physically closed.

**SRM status**
Displays the current mode of the Sub Ring manager.

Possible values:
- **manager**
  The Sub Ring port forwards data packets.
- **redundantManager**
  The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets.
- **singleManager**
  The Sub Ring is coupled to the base ring through one single device. This device blocks its Sub Ring port with the higher port number while the Sub Ring is physically closed.
- **disabled**
  The Sub Ring is inactive.

**Port status**
Displays the connection status of the Sub Ring port.

Possible values:
- **forwarding**
  The port is passing frames according to the forwarding behavior of IEEE 802.1D.
- **disabled**
  The port is dropping every frame.
- **blocked**
  The port is dropping every frame with the exception of the following cases:
  - The port passes frames used by the selected ring protocol specified to pass blocked ports.
  - The port passes frames from other protocols specified to pass blocked ports.
- **not-connected**
  The port link is down.

**VLAN**
Specifies the VLAN to which this Sub Ring is assigned. If no VLAN exists with the specified VLAN ID, then the device automatically creates it.

Possible values:
- **Available configured VLANs** (default setting: 0)
  If you do not want to use a separate VLAN for this Sub Ring, then you keep the value as 0.

**Partner MAC**
Displays the MAC address of the Sub Ring manager at the other end of the Sub Ring.
Mrp domain

Specifies the MRP domain of the Sub Ring manager. Assign the same MRP domain name to every member of a Sub Ring. If you only use Hirschmann devices, then you use the default value for the MRP domain; otherwise adjust this value if necessary. With multiple Sub Rings, the function lets you use the same MRP domain name for the Sub Rings.

Possible values:
- Permitted MRP domain names (default setting: 255.255.255.255.255.255.255.255)

Protocol

Specifies the protocol.

Possible values:
- iec-62439-mrp
6 Diagnostics

The menu contains the following dialogs:
- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- LLDP
- Loop Protection
- Report

6.1 Status Configuration

The menu contains the following dialogs:
- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)
6.1.1 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as error or ok in the Device status frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the Status tab and also in the Basic Settings > System dialog, Device status frame.

The dialog contains the following tabs:
- [Global]
- [Port]
- [Status]

[Global]

Device status

Displays the current status of the device. The device determines the status from the individual monitored parameters.

Possible values:
- ok
- error
  The device displays this value to indicate a detected error in one of the monitored parameters.

Traps

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function.

Possible values:
- marked (default setting)
  The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
  If the device detects a change in the monitored functions, then the device sends an SNMP trap.
- unmarked
  The sending of SNMP traps is inactive.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Connection errors

Activates/deactivates the monitoring of the link status of the port/interface.

Possible values:
- **marked**
  Monitoring is active.
  If the link interrupts on a monitored port/interface, then in the Device status frame, the value changes to **error**.
  In the Port tab, you have the option of selecting the ports/interfaces to be monitored individually.
- **unmarked** (default setting)
  Monitoring is inactive.

Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the temperature exceeds or falls below the specified threshold values, then in the Device status frame, the value changes to **error**.
- **unmarked**
  Monitoring is inactive.

You specify the temperature threshold values in the Basic Settings > System dialog, Upper temp. limit [°C] field and Lower temp. limit [°C] field.

Ethernet module removal

Activates/deactivates the monitoring of the modules.

Possible values:
- **marked**
  Monitoring is active.
  If you remove a module from the device, then in the Device status frame, the value changes to **error**.
  Further down, you have the option of selecting the modules to be monitored individually.
- **unmarked** (default setting)
  Monitoring is inactive.
External memory removal

Activates/deactivates the monitoring of the active external memory.

Possible values:

► marked
  Monitoring is active.
  If you remove the active external memory from the device, then in the Device status frame, the value changes to error.

► unmarked (default setting)
  Monitoring is inactive.

External memory not in sync

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

► marked
  Monitoring is active.
  In the Device status frame, the value changes to error in the following situations:
  – The configuration profile only exists in the device.
  – The configuration profile in the device differs from the configuration profile in the external memory.

► unmarked (default setting)
  Monitoring is inactive.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

► marked
  Monitoring is active.
  In the Device status frame, the value changes to error in the following situations:
  – The redundancy function becomes active (loss of redundancy reserve).
  – The device is a normal ring participant and detects an error in its settings.

► unmarked (default setting)
  Monitoring is inactive.

Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:

► marked (default setting)
  Monitoring is active.
  If the device has a detected power supply fault, then in the Device status frame, the value changes to error.

► unmarked
  Monitoring is inactive.
Ethernet module

Activates/deactivates the monitoring of this module.

Possible values:

- **marked**
  Monitoring is active.
  If you remove the module from the device, then in the Device status frame, the value changes to **error**.

- **unmarked** (default setting)
  Monitoring is inactive.
  This setting is effective when you mark the Ethernet module removal checkbox further up.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Propagate connection error

Activates/deactivates the monitoring of the link on the port/interface.

Possible values:

- **marked**
  Monitoring is active.
  If the link on the selected port/interface is interrupted, then in the Device status frame, the value changes to **error**.

- **unmarked** (default setting)
  Monitoring is inactive.
  This setting takes effect when you mark the Connection errors checkbox in the Global tab.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event in the format, Month Day, Year hh:mm:ss AM/PM.
Cause

Displays the event which caused the SNMP trap.
### 6.1.2 Security Status

This dialog gives you an overview of the status of the safety-relevant settings in the device.

The device displays its current status as **error** or **ok** in the *Security status* frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the *Status* tab and also in the *Basic Settings > System* dialog, *Security status* frame.

The dialog contains the following tabs:
- [Global]
- [Port]
- [Status]

#### [Global]

**Security status**

Displays the current status of the security-relevant settings in the device. The device determines the status from the individual monitored parameters.

Possible values:
- **ok**
- **error**
  
  The device displays this value to indicate a detected error in one of the monitored parameters.

#### Traps

**Send trap**

Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function.

Possible values:
- **marked**
  
  The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
  
  If the device detects a change in the monitored functions, then the device sends an SNMP trap.
- **unmarked** (default setting)
  
  The sending of SNMP traps is inactive.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Password default settings unchanged**

Activates/deactivates the monitoring of the password for the locally set up user account *admin*.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the password is set to the default setting for the *admin* user account, then in the *Security status* frame, the value changes to *error*.
- **unmarked**
  Monitoring is inactive.

You set the password in the *Device Security > User Management* dialog.

**Min. password length < 8**

Activates/deactivates the monitoring of the *Min. password length* policy.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the value for the *Min. password length* policy is less than 8, then in the *Security status* frame, the value changes to *error*.
- **unmarked**
  Monitoring is inactive.

You specify the *Min. password length* policy in the *Device Security > User Management* dialog in the *Configuration* frame.

**Password policy settings deactivated**

Activates/deactivates the monitoring of the Password policies settings.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the value for at least one of the following policies is less than 1, then in the *Security status* frame, the value changes to *error*.
  - *Upper-case characters (min.)*
  - *Lower-case characters (min.)*
  - *Digits (min.)*
  - *Special characters (min.)*
- **unmarked**
  Monitoring is inactive.

You specify the policy settings in the *Device Security > User Management* dialog in the *Password policy* frame.
User account password policy check deactivated

Activates/deactivates the monitoring of the Policy check function.

Possible values:

- **marked**  Monitoring is active.
  If the Policy check function is inactive for at least one user account, then in the Security status frame, the value changes to error.

- **unmarked** (default setting)  Monitoring is inactive.

You activate the Policy check function in the Device Security > User Management dialog.

Telnet server active

Activates/deactivates the monitoring of the Telnet server.

Possible values:

- **marked** (default setting)  Monitoring is active.
  If you enable the Telnet server, then in the Security status frame, the value changes to error.

- **unmarked**  Monitoring is inactive.

You enable/disable the Telnet server in the Device Security > Management Access > Server dialog, Telnet tab.

HTTP server active

Activates/deactivates the monitoring of the HTTP server.

Possible values:

- **marked** (default setting)  Monitoring is active.
  If you enable the HTTP server, then in the Security status frame, the value changes to error.

- **unmarked**  Monitoring is inactive.

You enable/disable the HTTP server in the Device Security > Management Access > Server dialog, HTTP tab.
SNMP unencrypted

Activates/deactivates the monitoring of the SNMP server.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If at least one of the following conditions applies, then in the **Security status** frame, the value changes to **error**:
  - The **SNMPv1** function is enabled.
  - The **SNMPv2** function is enabled.
  - The encryption for **SNMPv3** is disabled.
    You enable the encryption in the **Device Security > User Management** dialog, in the **SNMP encryption type** column.
- **unmarked**
  Monitoring is inactive.

You specify the settings for the SNMP agent in the **Device Security > Management Access > Server** dialog, **SNMP** tab.

Access to system monitor with serial interface possible

Activates/deactivates the monitoring of the system monitor.

When the system monitor is active, you have the possibility to change to the system monitor using a serial connection during the system startup.

Possible values:
- **marked**
  Monitoring is active.
  If you activate the system monitor, then in the **Security status** frame, the value changes to **error**.
- **unmarked** (default setting)
  Monitoring is inactive.

You activate/deactivate the system monitor in the **Diagnostics > System > Selftest** dialog.

Saving the configuration profile on the external memory possible

Activates/deactivates the monitoring of the configuration profile in the external memory.

Possible values:
- **marked**
  Monitoring is active.
  If you activate the saving of the configuration profile in the external memory, then in the **Security status** frame, the value changes to **error**.
- **unmarked** (default setting)
  Monitoring is inactive.

You activate/deactivate the saving of the configuration profile in the external memory in the **Basic Settings > External Memory** dialog.
Link interrupted on enabled device ports

Activates/deactivates the monitoring of the link on the active ports.

Possible values:

- marked
  Monitoring is active.
  If the link interrupts on an active port, then in the Security status frame, the value changes to error. In the Port tab, you have the option of selecting the ports to be monitored individually.

- unmarked (default setting)
  Monitoring is inactive.

Access with HiDiscovery possible

Activates/deactivates the monitoring of the HiDiscovery function.

Possible values:

- marked (default setting)
  Monitoring is active.
  If you enable the HiDiscovery function, then in the Security status frame, the value changes to error.

- unmarked
  Monitoring is inactive.

You enable/disable the HiDiscovery function in the Basic Settings > Network > Global dialog.

Load unencrypted config from external memory

Activates/deactivates the monitoring of loading unencrypted configuration profiles from the external memory.

Possible values:

- marked (default setting)
  Monitoring is active.
  If the settings allow the device to load an unencrypted configuration profile from the external memory, then in the Security status frame, the value changes to error.
  If the following preconditions are fulfilled, then the Security status frame in the Basic Settings > System dialog, displays an alarm.
    - The configuration profile stored in the external memory is unencrypted.
    - The Config priority column in the Basic Settings > External Memory dialog has the value first.

- unmarked
  Monitoring is inactive.
IEC61850-MMS active

Activates/deactivates the monitoring of the IEC61850-MMS function.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If you enable the IEC61850-MMS function, then in the Security status frame, the value changes to error.
- **unmarked**
  Monitoring is inactive.

You enable/disable the IEC61850-MMS function in the Advanced > Industrial Protocols > IEC61850-MMS dialog, Operation frame.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the HTTPS certificate.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the HTTPS server uses a self-created digital certificate, then in the Security status frame, the value changes to error.
- **unmarked**
  Monitoring is inactive.

Modbus TCP active

Activates/deactivates the monitoring of the Modbus TCP function.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If you enable the Modbus TCP function, then in the Security status frame, the value changes to error.
- **unmarked**
  Monitoring is inactive.

You enable/disable the Modbus TCP function in the Advanced > Industrial Protocols > Modbus TCP dialog, Operation frame.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
</table>

Displays the port number.
Link interrupted on enabled device ports

Activates/deactivates the monitoring of the link on the active ports.

Possible values:

► marked
  Monitoring is active.
  If the port is enabled (Basic Settings > Port dialog, Configuration tab, Port on checkbox is marked) and the link is down on the port, then in the Security status frame, the value changes to error.

► unmarked (default setting)
  Monitoring is inactive.

This setting takes effect when you mark the Link interrupted on enabled device ports checkbox in the Diagnostics > Status Configuration > Security Status dialog, Global tab.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event in the format, Month Day, Year hh:mm:ss AM/PM.

Cause

Displays the event which caused the SNMP trap.

6.1.3 Signal Contact

The signal contact is a potential-free relay contact. The device thus lets you perform remote diagnosis. The device uses the relay contact to signal the occurrence of events by opening the relay contact and interrupting the closed circuit.

Note: The device can contain several signal contacts. Each contact contains the same monitoring functions. Several contacts allow you to group various functions together providing flexibility in system monitoring.

The menu contains the following dialogs:

► Signal Contact 1 / Signal Contact 2
6.1.3.1 Signal Contact 1 / Signal Contact 2

In this dialog you specify the trigger conditions for the signal contact.

The signal contact gives you the following options:
- Monitoring the correct operation of the device.
- Signaling the device status of the device.
- Signaling the security status of the device.
- Controlling external devices by manually setting the signal contacts.

The device displays detected faults in the Status tab and also in the Basic Settings > System dialog, Signal contact status frame.

The dialog contains the following tabs:
- [Global]
- [Port]
- [Status]

[Global]

Configuration

Mode

Specifies which events the signal contact indicates.

Possible values:
- Manual setting (default setting for Signal Contact 2, if present)
  You use this setting to manually open or close the signal contact, for example to turn on or off a remote device. See the Contact option list.
- Monitoring correct operation (default setting)
  Using this setting the signal contact indicates the status of the parameters specified in the table below.
- Device status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status dialog. In addition, you can read the status in the Signal contact status frame.
- Security status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Security Status dialog. In addition, you can read the status in the Signal contact status frame.
- Device/Security status
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status and the Diagnostics > Status Configuration > Security Status dialog. In addition, you can read the status in the Signal contact status frame.
Contact

Toggles the signal contact manually. The prerequisite is that from the Mode drop-down list the Manual setting item is selected.

Possible values:
- **open**
  - The signal contact is opened.
- **close**
  - The signal contact is closed.

Signal contact status

Displays the current status of the signal contact.

Possible values:
- **Opened (error)**
  - The signal contact is opened. The circuit is interrupted.
- **Closed (ok)**
  - The signal contact is closed. The circuit is closed.

Trap configuration

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function.

Possible values:
- **marked**
  - The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
  - If the device detects a change in the monitored functions, then the device sends an SNMP trap.
- **unmarked** (default setting)
  - The sending of SNMP traps is inactive.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Connection errors

Activates/deactivates the monitoring of the link status of the port/interface.

Possible values:
- **marked**
  Monitoring is active.
  If the link interrupts on a monitored port/interface, then the signal contact opens.
  In the Port tab, you have the option of selecting the ports/interfaces to be monitored individually.
- **unmarked** (default setting)
  Monitoring is inactive.

Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the temperature exceeds or falls below the specified threshold values, then the signal contact opens.
- **unmarked**
  Monitoring is inactive.

You specify the temperature threshold values in the Basic Settings > System dialog, Upper temp. limit [°C] field and Lower temp. limit [°C] field.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:
- **marked**
  Monitoring is active.
  The signal contact opens in the following situations:
  - The redundancy function becomes active (loss of redundancy reserve).
  - The device is a normal ring participant and detects an error in its settings.
- **unmarked** (default setting)
  Monitoring is inactive.

Ethernet module removal

Activates/deactivates the monitoring of the modules.

Possible values:
- **marked**
  Monitoring is active.
  If you remove a module from the device, then the signal contact opens.
  Further down, you have the option of selecting the modules to be monitored individually.
- **unmarked** (default setting)
  Monitoring is inactive.
External memory removed

Activates/deactivates the monitoring of the active external memory.

Possible values:
- **marked**
  Monitoring is active.
  If you remove the active external memory from the device, then the signal contact opens.
- **unmarked** (default setting)
  Monitoring is inactive.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:
- **marked**
  Monitoring is active.
  The signal contact opens in the following situations:
  - The configuration profile only exists in the device.
  - The configuration profile in the device differs from the configuration profile in the external memory.
- **unmarked** (default setting)
  Monitoring is inactive.

Ethernet loops

Activates/deactivates the monitoring of layer 2 Ethernet loops. You specify the settings for the Loop Protection function in the Diagnostics > Loop Protection dialog.

Possible values:
- **marked**
  Monitoring is active.
  If the device has detected an Ethernet loop, then the signal contact opens.
- **unmarked** (default setting)
  Monitoring is inactive.

Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:
- **marked** (default setting)
  Monitoring is active.
  If the device has a detected power supply fault, then the signal contact opens.
- **unmarked**
  Monitoring is inactive.
Ethernet module

Activates/deactivates the monitoring of this module.

Possible values:

- marked
  Monitoring is active.
  If you remove this module from the device, then the signal contact opens.

- unmarked (default setting)
  Monitoring is inactive.

This setting is effective when you mark the Ethernet module removal checkbox further up.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Propagate connection error

Activates/deactivates the monitoring of the link on the port/interface.

Possible values:

- marked
  Monitoring is active.
  If the link interrupts on the selected port/interface, then the signal contact opens.

- unmarked (default setting)
  Monitoring is inactive.

This setting takes effect when you mark the Connection errors checkbox in the Global tab.

[Status]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Timestamp

Displays the date and time of the event in the format, Month Day, Year  hh:mm:ss AM/PM.
Cause

Displays the event which caused the SNMP trap.

6.1.4 MAC Notification

The device lets you track changes in the network using the MAC address of the devices in the network. The device saves the combination of port and MAC address in its MAC address table. If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap.

This function is intended for ports to which you connect end devices and thus the MAC address changes infrequently.

Operation

Enables/disables the MAC Notification function in the device.

Possible values:
- **On**
  - The MAC Notification function is enabled.
- **Off** (default setting)
  - The MAC Notification function is disabled.

Configuration

Interval [s]

Specifies the send interval in seconds. If the device (un)learns the MAC address of a (dis)connected device, then the device sends an SNMP trap after this time.

Possible values:
- **0..2147483647** (default setting: 1)

Before sending an SNMP trap, the device registers up to 20 MAC addresses. If the device detects a high number of changes, then the device sends the SNMP trap before the send interval expires.
### Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activates/deactivates the MAC Notification function on the port.</td>
</tr>
<tr>
<td>Possible values:</td>
<td></td>
</tr>
</tbody>
</table>
| ▶ marked | The MAC Notification function is active on the port. The device sends an SNMP trap in case of one of the following events:  
- The device learns the MAC address of a newly connected device.  
- The device unlearns the MAC address of a disconnected device. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified. |
| ▶ unmarked (default setting) | The MAC Notification function is inactive on the port. |
| Last MAC address | Displays the MAC address of the device last connected on or disconnected from the port.  
The device detects the MAC addresses of devices which are connected as follows:  
- directly connected to the port  
- connected to the port through other devices in the network |
| Last MAC status | Displays the status of the Last MAC address value on this port. |
| Possible values: |
| ▶ added | The device detected that another device was connected at the port. |
| ▶ removed | The device detected that the connected device was removed from the port. |
| ▶ other | The device did not detect a status. |
6.1.5 **Alarms (Traps)**

The device lets you send an SNMP trap as a reaction to specific events. In this dialog you specify the trap destinations to which the device sends the SNMP traps.

The events for which the device triggers an SNMP trap, you specify, for example, in the following dialogs:
- in the [Diagnostics > Status Configuration > Device Status](#) dialog
- in the [Diagnostics > Status Configuration > Security Status](#) dialog
- in the [Diagnostics > Status Configuration > MAC Notification](#) dialog

**Operation**

Enables/disables the sending of SNMP traps to the trap destinations.

Possible values:
- **On** (default setting)
  - The sending of SNMP traps is enabled.
- **Off**
  - The sending of SNMP traps is disabled.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

Add

Opens the Create window to add a table row.
- In the Name field you specify a name for the trap destination.
- In the Address field you specify the IP address and the port number of the trap destination. If you choose not to enter a port number, then the device automatically adds the port number 162.

Remove

Removes the selected table row.
Name

Specifies the name of the trap destination.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters

Address

Specifies the IP address and the port number of the trap destination.

Possible values:
- `<Valid IPv4 address>:<port number>`

Active

Activates/deactivates the sending of SNMP traps to this trap destination.

Possible values:
- **marked** (default setting)
  - The sending of SNMP traps to this trap destination is active.
- **unmarked**
  - The sending of SNMP traps to this trap destination is inactive.
6.2 System

The menu contains the following dialogs:
- System Information
- Hardware State
- Configuration Check
- IP Address Conflict Detection
- ARP
- Selftest
6.2.1 System Information

This dialog displays the current operating condition of individual components in the device. The displayed values are a snapshot; they represent the operating condition at the time the dialog was loaded to the page.

Buttons

Save system information

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.
6.2.2 **Hardware State**

This dialog provides information about the distribution and state of the flash memory of the device.

**Information**

Operating hours

Displays the total operating time of the device since it was delivered.

Possible values:

```
...d ..h ..m ..s
```

Day(s) Hour(s) Minute(s) Second(s)

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Flash region

Displays the name of the parameter, for example for the relevant memory area.

Description

Displays a description for the parameter.

Flash sectors

Displays how many sectors are assigned to the memory area.

Sector erase operations

Displays how many times the device has overwritten the sectors of the memory area.
6.2.3 **Configuration Check**

The device lets you compare the settings in the device with the settings in its neighboring devices. For this purpose, the device uses the information that it received from its neighboring devices through topology recognition (LLDP).

The dialog lists the detected deviations, which affect the performance of the communication between the device and the recognized neighboring devices. When the table remains empty, the configuration check was successful and the settings in the device are compatible with the settings in the detected neighboring devices. You update the content of the table by clicking the **button.

**Note:** A neighboring device without LLDP support, which forwards LLDP packets, can be the cause of equivocal messages in the dialog. This occurs if the neighboring device is a hub or a switch without management, which ignores the IEEE 802.1D-2004 standard. In this case, the dialog displays the devices recognized and connected to the neighboring device as connected to the device itself, even though they are connected to the neighboring device.

**Information**

When you click the **button in the Banner, a tooltip displays the summary of the information in this frame.

**Error**

Displays the number of **ERROR** level deviations that the device detected during the configuration check.

**Warning**

Displays the number of **WARNING** level deviations that the device detected during the configuration check.

If you have set up more than 39 VLANs in the device, then the dialog continuously displays a warning. The reason is the limited number of possible VLAN data sets in LLDP packets with a maximum length. The device compares the first 39 VLANs automatically. If you have set up 40 or more VLANs in the device, then check the congruence of the further VLANs manually, if necessary.

**Information**

Displays the number of **INFORMATION** level deviations that the device detected during the configuration check.
Table

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

Displays detailed information about the detected deviations in the area below the table row. To hide the detailed information again, click the button. If you click the icon in the table header, you display or hide the detailed information for each table row.

ID

Displays the rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.

Level

Displays the level of deviation between the settings in this device and the settings in the detected neighboring devices.

The device differentiates between the following access statuses:

- **INFORMATION**
  The performance of the communication between the two devices is not impaired.

- **WARNING**
  The performance of the communication between the two devices is possibly impaired.

- **ERROR**
  The communication between the two devices is impaired.

Message

Displays a summary of the detected deviations.
6.2.4 **IP Address Conflict Detection**

Using the *IP Address Conflict Detection* function the device verifies that its IP address is unique in the network. For this purpose, the device analyzes received ARP packets.

In this dialog you specify the procedure with which the device detects address conflicts and specify the required settings for this.

The device displays detected address conflicts in the table.

When the device detects an address conflict, the status LED of the device flashes red 4 times.

**Operation**

Enables/disables the *IP Address Conflict Detection* function.

Possible values:

- **On** (default setting)
  
  The *IP Address Conflict Detection* function is enabled. The device verifies that its IP address is unique in the network.

- **Off**
  
  The *IP Address Conflict Detection* function is disabled.

**Information**

Conflict detected

Displays if an address conflict currently exists.

Possible values:

- **marked**
  
  The device detects an address conflict.

- **unmarked**
  
  The device does not detect an address conflict.

**Configuration**

Detection mode

Specifies the procedure with which the device detects address conflicts.

Possible values:

- **active and passive** (default setting)
  
  The device uses active and passive address conflict detection.
Active address conflict detection. The device actively helps avoid communicating with an IP address that already exists in the network. The address conflict detection begins as soon as you connect the device to the network or change its IP parameters.

- The device sends 4 ARP probe data packets at the interval specified in the Detection delay [ms] field. If the device receives a response to these data packets, then there is an address conflict.
- If the device does not detect an address conflict, then it sends 2 gratuitous ARP data packets as an announcement. The device also sends these data packets when the address conflict detection is disabled.
- If the IP address already exists in the network, then the device changes back to the previously used IP parameters (if possible). If the device receives its IP parameters from a DHCP server, then it sends a DHCPDECLINE message back to the DHCP server.
- After the period specified in the Release delay [s] field, the device checks if the address conflict still exists. When the device detects 10 address conflicts one after the other, the device extends the waiting time to 60 s for the next check.
- When the device resolves the address conflict, the device management returns to the network again.

Passive address conflict detection. The device analyzes the data stream in the network. If another device in the network is using the same IP address, then the device initially “defends” its IP address. The device stops sending if the other device keeps sending with the same IP address.

- As a “defence” the device sends gratuitous ARP data packets. The device repeats this procedure for the number of times specified in the Address protections field.
- If the other device continues sending with the same IP address, then after the period specified in the Release delay [s] field, the device periodically checks if the address conflict still exists.
- When the device resolves the address conflict, the device management returns to the network again.

Send periodic ARP probes

Activates/deactivates the periodic address conflict detection.

Possible values:

- **marked** (default setting)
  The periodic address conflict detection is active.
  - The device periodically sends an ARP probe data packet every 90 to 150 seconds and waits for the time specified in the Detection delay [ms] field for a response.
  - If the device detects an address conflict, then the device applies the passive detection mode function. If the Send trap function is active, then the device sends an SNMP trap.
- **unmarked**
  The periodic address conflict detection is inactive.
**Detection delay [ms]**

Specifies the period in milliseconds for which the device waits for a response after sending a ARP data packets.

Possible values:

- **20..500** (default setting: 200)

**Release delay [s]**

Specifies the period in seconds after which the device checks again if the address conflict still exists.

Possible values:

- **3..3600** (default setting: 15)

**Address protections**

Specifies how many times the device sends gratuitous ARP data packets in the passive detection mode to “defend” its IP address.

Possible values:

- **0..100** (default setting: 1)

**Protection interval [ms]**

Specifies the period in milliseconds after which the device sends gratuitous ARP data packets again in the passive detection mode to “defend” its IP address.

Possible values:

- **20..10000** (default setting: 10000)

**Send trap**

Activates/deactivates the sending of SNMP traps when the device detects an address conflict.

Possible values:

- **marked**
  - The sending of SNMP traps is active. The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
  - If the device detects an address conflict, then the device sends an SNMP trap.

- **unmarked** (default setting)
  - The sending of SNMP traps is inactive.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Timestamp**

Displays the time at which the device detected an address conflict.
Port

Displays the number of the port on which the device detected the address conflict.

IP address

Displays the IP address that is causing the address conflict.

MAC address

Displays the MAC address of the device with which the address conflict exists.
6.2.5 ARP

This dialog displays the MAC and IP addresses of the neighboring devices connected to the device management.

The device can display both IPv4 and IPv6 addresses. For the IPv6 protocol, addresses of the neighboring devices are obtained with the use of the Neighbor Discovery Protocol (NDP).

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

- Reset ARP table
  Removes the dynamically set up addresses from the ARP table.

Port

- Displays the port number.

IP address

- Displays the IPv4 address or the IPv6 address of a neighboring device.

MAC address

- Displays the MAC address of a neighboring device.

Last updated

- Displays the time in seconds since the current settings of the entry were registered in the ARP table.

Type

- Displays the type of the entry.

Possible values:

- **static**
  Static entry. When the ARP table is deleted, the device keeps the static entry.

- **dynamic**
  Dynamic entry. When the Aging time [s] has been exceeded and the device does not receive any data from this device during this time, the device deletes the dynamic entry.

- **local**
  IP and MAC address of the device management.
Displays that the ARP table contains the IP/MAC address assignment as an active entry.
6.2.6 Selftest

This dialog lets you do the following:
- Activate/deactivate the RAM test when the device is being started.
- Activate/deactivate the option of changing to the system monitor during the system startup.
- Specify how the device behaves in the case of a detected error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings block your access to the device permanently.
- **SysMon1 is available** checkbox is unmarked.
- **Load default config on error** checkbox is unmarked.

This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

RAM test

Activates/deactivates the RAM memory check during the system startup.

Possible values:
- **marked** (default setting)
  - The RAM memory check is activated. During the system startup, the device checks the RAM memory.
- **unmarked**
  - The RAM memory check is deactivated. This shortens the start time for the device.

SysMon1 is available

Activates/deactivates the option of changing to the system monitor during the system startup.

Possible values:
- **marked** (default setting)
  - The device lets you change to the system monitor during the system startup.
- **unmarked**
  - The device starts without the option of changing to the system monitor.

Among other things, the system monitor lets you update the device software and to delete saved configuration profiles.
Load default config on error

Activates/deactivates the loading of the default settings if the device does not detect any readable configuration profile when restarting.

Possible values:
- **marked** (default setting)
  - The device loads the default settings.
- **unmarked**
  - The device interrupts the restart and stops. The access to the device management is possible only using the Command Line Interface through the serial interface.
  - To regain the access to the device through the network, open the system monitor and reset the settings. During the system startup, the device loads the default settings.

**Table**

In this table you specify how the device behaves in the case of a detected error.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Cause**

Detected error causes to which the device reacts.

Possible values:
- **task**
  - The device detects errors in the applications executed, for example if a task terminates or is not available.
- **resource**
  - The device detects errors in the resources available, for example if the memory is becoming scarce.
- **software**
  - The device detects software errors, for example error in the consistency check.
- **hardware**
  - The device detects hardware errors, for example in the chip set.

**Action**

Specifies how the device behaves if the adjacent event occurs.

Possible values:
- **logOnly**
  - The device registers the detected error in the log file. See the Diagnostics > Report > System Log dialog.
- **sendTrap**
  - The device sends an SNMP trap.
  - The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.
- **reboot** (default setting)
  - The device triggers a restart.
6.3 Email Notification

The device lets you inform multiple recipients by email about events that have occurred.

The device sends the emails immediately or periodically depending on the event severity. Usually you specify events with a high severity to be sent immediately.

You can specify multiple recipients to which the device sends the emails either immediately or periodically.

The menu contains the following dialogs:
- Email Notification Global
- Email Notification Recipients
- Email Notification Mail Server
6.3.1 Email Notification Global

In this dialog you specify the sender settings. Also, you specify for which event severities the device sends the emails immediately and for which periodically.

**Operation**

Enables/disables the sending of emails:

Possible values:

- **On**
  - The sending of emails is enabled.
- **Off** (default setting)
  - The sending of emails is disabled.

**Information**

**Buttons**

- **Clear email notification statistics**
  
  Resets the counters in the *Information* frame to 0.

**Sent messages**

Displays how many times the device has successfully sent an email to the mail server.

**Undeliverable messages**

Displays how many times the device has unsuccessfully tried to send an email to the mail server.

**Time of the last messages sent**

Displays the date and time at which the device has last sent an email to the mail server.

**Certificate**

The device can send messages to a server over unsecured networks. To help deny a “man in the middle” attack, request that the Certificate Authority (CA) creates a certificate for the server.

Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the settings for the mail servers, then use the IP address or DNS name provided as **Common Name** or **Subject Alternative Name** in the certificate. Otherwise the certificate validation will be unsuccessful.
URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:
- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
  
  ```
  -----BEGIN CERTIFICATE-----
  and
  -----END CERTIFICATE-----
  ```

For security reason, we recommend to constantly use a certificate which is signed by a certification authority.

The device gives you the following options for copying the certificate to the device:
- **Import from the PC**
  When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
- **Import from an FTP server**
  When the certificate is on a FTP server, specify the URL for the file in the following form:
  
  `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`

- **Import from a TFTP server**
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  
  `tftp://<IP address>/<path>/<file name>`

- **Import from an SCP or SFTP server**
  When the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:
  
  - `scp:// or sftp://<IP address>/<path>/<file name>`
  - When you click the Start button, the device displays the Credentials window. There you enter **User name** and **Password**, to log in to the server.
  - `scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copies the certificate specified in the **URL** field to the device.

**Sender**

Specifies the email address of the device.

The device sends the emails using this email address as the sender.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters
  (default setting: `switch@hirschmann.com`)
Notification immediate

Here you specify the settings for emails which the device sends immediately.

Severity

Specifies the minimum severity of events for which the device immediately sends an email. If an event of this severity occurs, or of a more urgent severity, then the device sends an email to the recipients.

Possible values:
- emergency
- alert (default setting)
- critical
- error
- warning
- notice
- informational
- debug

Subject

Specifies the subject of the email.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

Notification periodic

Here you specify the settings for emails which the device sends periodically.

Severity

Specifies the minimum severity of events for which the device periodically sends an email. If an event of this severity occurs, or of a more urgent severity, then the device registers the event in the buffer. The device sends the buffer content periodically or when the buffer overflows.

If an event of a less urgent severity occurs, then the device does not register the event in the buffer.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug
Subject

Specifies the subject of the email.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

Sending interval [min]

Specifies the send interval in minutes.

If the device has registered at least one event, then the device sends an email with the log file after the time expires.

Possible values:
- 30..1440 (default setting: 30)

Send

Sends an email immediately with the buffer content and clears the buffer.

Meaning of the event severities

<table>
<thead>
<tr>
<th>Severity</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>Device not ready for operation</td>
</tr>
<tr>
<td>alert</td>
<td>Immediate user intervention required</td>
</tr>
<tr>
<td>critical</td>
<td>Critical status</td>
</tr>
<tr>
<td>error</td>
<td>Error status</td>
</tr>
<tr>
<td>warning</td>
<td>Warning</td>
</tr>
<tr>
<td>notice</td>
<td>Significant, normal status</td>
</tr>
<tr>
<td>informational</td>
<td>Informal message</td>
</tr>
<tr>
<td>debug</td>
<td>Debug message</td>
</tr>
</tbody>
</table>
6.3.2 Email Notification Recipients

In this dialog you specify the recipients to which the device sends the emails. The device lets you specify up to 10 recipients.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

Notification type

Specifies if the device sends the emails to this recipient immediately or periodically.

Possible values:

- **immediate**
  
  The device sends the emails to this recipient immediately.

- **periodic**
  
  The device sends the emails to this recipient periodically.
Diagnostics

[ Diagnostics > Email Notification > Recipients ]

Address

Specifies the email address of the recipient.

Possible values:
- Valid email address with up to 255 characters

Active

Activates/deactivates the informing of the recipient.

Possible values:
- marked
  The informing of the recipient is active.
- unmarked (default setting)
  The informing of the recipient is inactive.
6.3.3 **Email Notification Mail Server**

In this dialog you specify the settings for the mail servers. The device supports encrypted and unencrypted connections to the mail server.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  Adds a table row.

- **Remove**
  Removes the selected table row.

- **Connection test**
  Opens the Connection test window to send a test email.

  If the mail server settings are correct, then the selected recipients receive a test email.

  - In the **Recipient** field, you specify to which recipients the device sends the test email:
    - **Immediate**
      The device sends the test email to the recipients to which the device sends emails immediately.
    - **Periodic**
      The device sends the test email to the recipients to which the device sends emails periodically.

  - In the **Message text** field, you specify the text of the test email.

**Index**

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Description

Specifies the name of the server.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

IP address

Specifies the IP address or the DNS name of the server.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)
- DNS name in the format domain.tld or host.domain.tld
  
  If you specify a DNS name, then also enable the Client function in the Advanced > DNS > Client > Global dialog.
  
  If you establish encrypted connections using the certificate, then verify that the DNS name is equal to the server DNS name mentioned in the certificate.

Destination TCP port

Specifies the TCP port of the server.

Possible values:
- 1..65535 (default setting: 25)
  
  Exception: Port 2222 is reserved for internal functions.

Frequently used TCP-Ports:
- SMTP 25
- Message Submission 587

Encryption

Specifies the protocol which encrypts the connection between the device and the mail server.

Possible values:
- none (default setting)
  
  The device establishes an an unencrypted connection to the server.
- tlsv1
  
  The device establishes an encrypted connection to the server using the startTLS extension.
User name

Specifies the user name of the account which the device uses to authenticate on the mail server.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

Password

Specifies the password of the account which the device uses to authenticate on the mail server.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

Timeout [s]

Specifies the time in seconds after which the device sends an email again. The prerequisite is that the device was unsuccessful at sending the complete email due to a connection error.

Possible values:
- 1..15 (default setting: 3)

Active

Activates/deactivates the use of the mail server.

Possible values:
- marked
  The mail server is active.
  The device sends emails to this mail server.
- unmarked (default setting)
  The mail server is inactive.
  The device does not send emails to this mail server.

6.4 Syslog

The device lets you report selected events, independent of the severity of the event, to different syslog servers. In this dialog you specify the settings for this function and manage up to 8 syslog servers.
Operation

Enables/disables the sending of events to the syslog servers.

Possible values:

- **On**
  - The sending of events is enabled.
  - The device sends the events specified in the table to the specified syslog servers.

- **Off** (default setting)
  - The sending of events is disabled.

Certificate

The device can send messages to a server over unsecured networks. To help deny a "man in the middle" attack, request that the Certificate Authority (CA) creates a certificate for the server. Configure the server to use the certificate. Transfer the certificate onto the device.

If you specify the parameters on the server, then verify that you specify the IP address and DNS name provided in the certificate as the Common Name or Subject Alternative Name. Otherwise the certificate validation will be unsuccessful.

**Note:** In order for the changes to take effect after loading a new certificate, restart the Syslog function.

URL

Specifies the path and file name of the certificate.

The device accepts certificates with the following properties:

- X.509 format
- .PEM file name extension
- Base64-coded, enclosed by
  
  `-----BEGIN CERTIFICATE-----`

  and

  `-----END CERTIFICATE-----`

For security reason, we recommend to constantly use a certificate which is signed by a certification authority.

The device gives you the following options for copying the certificate to the device:

- **Import from the PC**
  - When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.

- **Import from an FTP server**
  - When the certificate is on a FTP server, specify the URL for the file in the following form:

    `ftp://<user>:<password>@<IP address>:<port>/<path>/<file name>`
- Import from a TFTP server
  When the certificate is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`

- Import from an SCP or SFTP server
  When the certificate is on an SCP or SFTP server, you specify the URL for the file in the following form:
  - `scp://<IP address>/<path>/<file name>`
    When you click the Start button, the device displays the Credentials window. There you enter User name and Password, to log in to the server.
  - `sftp://<user>:<password>@<IP address>/<path>/<file name>`

Start

Copies the certificate specified in the URL field to the device.

Table

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

Buttons

- Add
  Adds a table row.

- Remove
  Removes the selected table row.

Index

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

When you delete a table row, this leaves a gap in the numbering. When you create a new table row, the device fills the first gap.

Possible values:

- 1..8

IP address

Specifies the IP address of the syslog server.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)
- Valid IPv6 address
- Hostname
Destination UDP port

Specifies the TCP or UDP port on which the syslog server expects the log entries.

Possible values:
- 1..65535 (default setting: 514)

Transport type

Specifies the transport type the device uses to send the events to the syslog server.

Possible values:
- udp (default setting)
The device sends the events over the UDP port specified in the Destination UDP port column.
- tls
The device sends the events over TLS on the TCP port specified in the Destination UDP port column.

Min. severity

Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug

Type

Specifies the type of the log entry transmitted by the device.

Possible values:
- systemlog (default setting)
- audittrail

Active

Activates/deactivates the transmission of events to the syslog server:
- marked
  The device sends events to the syslog server.
- unmarked (default setting)
  The transmission of events to the syslog server is deactivated.
6.5  **Ports**

The menu contains the following dialogs:

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring
This dialog lets you look at the SFP transceivers currently connected to the device and their properties.

### Table

The table displays valid values if the device is equipped with SFP transceivers.

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module type</td>
<td>Type of the SFP transceiver, for example M-SFP-SX/LC.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Displays the serial number of the SFP transceiver.</td>
</tr>
<tr>
<td>Connector type</td>
<td>Displays the connector type.</td>
</tr>
<tr>
<td>Supported</td>
<td>Displays if the device supports the SFP transceiver.</td>
</tr>
<tr>
<td>Temperature [°C]</td>
<td>Operating temperature of the SFP transceiver in °Celsius.</td>
</tr>
<tr>
<td>Tx power [mW]</td>
<td>Transmission power of the SFP transceiver in mW.</td>
</tr>
<tr>
<td>Rx power [mW]</td>
<td>Receiving power of the SFP transceiver in mW.</td>
</tr>
<tr>
<td>Tx power [dBm]</td>
<td>Transmission power of the SFP transceiver in dBm.</td>
</tr>
<tr>
<td>Rx power [dBm]</td>
<td>Receiving power of the SFP transceiver in dBm.</td>
</tr>
</tbody>
</table>
6.5.2 TP cable diagnosis

This feature tests the cable attached to an interface for short or open circuit. The table displays the
cable status and estimated length. The device also displays the individual cable pairs connected to
the port. When the device detects a short circuit or an open circuit in the cable, it also displays the
estimated distance to the problem.

To receive dependable results, use the TP cable diagnosis function for twisted pair cables with a
minimum length of 3 meters.

Note: This test temporarily interrupts the data stream on the port.

Information

Port

Displays the port number.

Start cable diagnosis...

Opens the Select port window.

From the Port drop-down list you select the port to be tested. Use for copper-based ports only.

To initiate the cable test on the selected port, click the Ok button.

Status

Status of the Virtual Cable Tester.

Possible values:

- active
  Cable testing is in progress.
  To start the test, click the Start cable diagnosis.. button. This action opens the Select port window.

- success
  The device displays this entry after performing a successful test.

- failure
  The device displays this entry after an interruption in the test.

- uninitialized
  The device displays this entry while in standby.
## Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Cable pair</th>
<th>Displays the cable pair to which this table row relates. The device uses the first PHY index supported to display the values.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>Displays the results of the cable test.</th>
</tr>
</thead>
</table>

### Possible values:

- **normal**
  - The cable is functioning properly.
- **open**
  - There is a break in the cable causing an interruption.
- **short**
  - Wires in the cable are touching together causing a short circuit.
- **unknown**
  - The device displays this value for untested cable pairs.

The device displays different values than expected in the following cases:

- If no cable is connected to the port, then the device displays the value **unknown** instead of **open**.
- If the port is inactive, then the device displays the value **short**.

<table>
<thead>
<tr>
<th>Min. length</th>
<th>Displays the minimum estimated length of the cable in meters.</th>
</tr>
</thead>
</table>

If the cable length is unknown or in the **Information** frame the **Status** field displays the value **active**, **failure** or **uninitialized**, then the device displays the value **0**.

<table>
<thead>
<tr>
<th>Max. length</th>
<th>Displays the maximum estimated length of the cable in meters.</th>
</tr>
</thead>
</table>

If the cable length is unknown or in the **Information** frame the **Status** field displays the value **active**, **failure** or **uninitialized**, then the device displays the value **0**.

<table>
<thead>
<tr>
<th>Distance [m]</th>
<th>Displays the estimated distance in meters from one end of the cable to the other or to an interruption in the cable.</th>
</tr>
</thead>
</table>

If the cable length is unknown or in the **Information** frame the **Status** field displays the value **active**, **failure** or **uninitialized**, then the device displays the value **0**.
6.5.3 Port Monitor

The Port Monitor function monitors the adherence to the specified parameters on the ports. If the Port Monitor function detects that the parameters are being exceeded, then the device performs an action.

To apply the Port Monitor function, perform the following steps:

- **Global tab**
  - Enable the Port Monitor function in the Operation frame.
  - Activate for each port those parameters that you want the Port Monitor function to monitor.
- **Link flap, CRC/Fragments and Overload detection tabs**
  - Specify the threshold values for the parameters for each port.
- **Link speed/Duplex mode detection tab**
  - Activate the allowed combinations of speed and duplex mode for each port.
- **Global tab**
  - Specify for each port an action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.
- **Auto-disable tab**
  - Mark the Auto-disable checkbox for the monitored parameters if you have specified the auto-disable action at least once.

The dialog contains the following tabs:

- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

[Global]

In this tab you enable the Port Monitor function and specify the parameters that the Port Monitor function is monitoring. Also specify the action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.

**Operation**

Enables/disables the Port Monitor function globally.

Possible values:

- **On**
  - The Port Monitor function is enabled.
- **Off** (default setting)
  - The Port Monitor function is disabled.
Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Reset

Opens the Which statistic should be deleted? window. The window displays the ports that you can enable again and reset the related counters to 0. Click and select a table row to enable the corresponding port again.

This affects the counters in the following dialogs:

- Diagnostics > Ports > Port Monitor dialog
  - Link flap tab
  - CRC/Fragments tab
  - Overload detection tab
- Diagnostics > Ports > Auto-Disable dialog

Port

Displays the port number.

Link flap on

Activates/deactivates the monitoring of link flaps on the port.

Possible values:

- marked
  Monitoring is active.
  - The Port Monitor function monitors link flaps on the port.
  - If the device detects too many link flaps, then the device executes the action specified in the Action column.
  - On the Link flap tab, specify the parameters to be monitored.
- unmarked (default setting)
  Monitoring is inactive.

CRC/Fragments on

Activates/deactivates the monitoring of CRC/fragment errors detected on the port.

Possible values:

- marked
  Monitoring is active.
  - The Port Monitor function monitors CRC/fragment errors detected on the port.
  - If the device detects too many CRC/fragment errors, then the device executes the action specified in the Action column.
  - On the CRC/Fragments tab, specify the parameters to be monitored.
- unmarked (default setting)
  Monitoring is inactive.
**Duplex mismatch detection active**

Activates/deactivates the monitoring of duplex mismatches on the port.

Possible values:

- `marked`
  - Monitoring is active.
  - The *Port Monitor* function monitors duplex mismatches on the port.
  - If the device detects a duplex mismatch, then the device executes the action specified in the *Action* column.

- `unmarked` (default setting)
  - Monitoring is inactive.

**Overload detection on**

Activates/deactivates the overload detection on the port.

Possible values:

- `marked`
  - Monitoring is active.
  - The *Port Monitor* function monitors the data load on the port.
  - If the device detects a data overload on the port, then the device executes the action specified in the *Action* column.
  - On the *Overload detection* tab, specify the parameters to be monitored.

- `unmarked` (default setting)
  - Monitoring is inactive.

**Link speed/Duplex mode detection on**

Activates/deactivates the monitoring of the link speed and duplex mode on the port.

Possible values:

- `marked`
  - Monitoring is active.
  - The *Port Monitor* function monitors the link speed and duplex mode on the port.
  - If the device detects an unpermitted combination of link speed and duplex mode, then the device executes the action specified in the *Action* column.
  - On the *Link speed/Duplex mode detection* tab, specify the parameters to be monitored.

- `unmarked` (default setting)
  - Monitoring is inactive.

**Active condition**

Displays the monitored parameter that led to the action on the port.

Possible values:

- `Link flap`
  - Too many link changes during the observed period.

- `CRC/Fragments`
  - Too many CRC/fragment errors detected during the observed period.

- `Duplex mismatch`
  - Duplex mismatch detected.
Overload detection
Overload detected during the observed period.

Link speed/Duplex mode detection
Impermissible combination of speed and duplex mode detected.

Action

Specifies the action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.

Possible values:

- **disable port**
  The device disables the port and sends an SNMP trap.
  The Link status LED for the port flashes 3× per period.
  - To re-enable the port, select the table row of the port, click the button.
  - If the parameters are no longer being exceeded, then the Auto-Disable function enables the relevant port again after the specified waiting period. The prerequisite is that on the Auto-disable tab the checkbox for the monitored parameter is marked.

- **send trap**
  The device sends an SNMP trap.
  The prerequisite is that in the Diagnostics > Status Configuration > Alarms (Traps) dialog the Alarms (Traps) function is enabled and at least one trap destination is specified.

- **auto-disable** (default setting)
  The device disables the port and sends an SNMP trap.
  The Link status LED for the port flashes 3× per period.
  The prerequisite is that on the Auto-disable tab the checkbox for the monitored parameter is marked.
  - The Diagnostics > Ports > Auto-Disable dialog displays which ports are currently disabled due to the parameters being exceeded.
  - After a waiting period, the Auto-Disable function enables the port again automatically. For this you go to the Diagnostics > Ports > Auto-Disable dialog and specify a waiting period for the relevant port in the Reset timer [s] column.

Port status

Displays the operating state of the port.

Possible values:

- **up**
  The port is enabled.

- **down**
  The port is disabled.

- **notPresent**
  Physical port unavailable.

[Auto-disable]

In this tab you activate the Auto-Disable function for the parameters monitored by the Port Monitor function.
**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Reason**

Displays the parameters monitored by the Port Monitor function.

Mark the adjacent checkbox so that the Port Monitor function carries out the auto-disable action if it detects that the monitored parameters have been exceeded.

**Auto-disable**

Activates/deactivates the Auto-Disable function for the adjacent parameters.

Possible values:

- marked
  - The Auto-Disable function for the adjacent parameters is active.
  - If the adjacent parameters are exceeded and the value auto-disable is specified in the Action column, then the device carries out the Auto-Disable function.

- unmarked (default setting)
  - The Auto-Disable function for the adjacent parameters is inactive.

**Link flap**

In this tab you specify individually for every port the following settings:

- The number of link changes.
- The period during which the Port Monitor function monitors a parameter to detect discrepancies.

You also see how many link changes the Port Monitor function has detected up to now.

The Port Monitor function monitors those ports for which the checkbox in the Link flap on column is marked on the Global tab.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Port**

Displays the port number.
Diagnostics

[ Diagnostics > Ports > Port Monitor ]

Sampling interval [s]

Specifies in seconds, the period during which the Port Monitor function monitors a parameter to detect discrepancies.

Possible values:

- 1..180  (default setting: 10)

Link flaps

Specifies the number of link changes.

If the Port Monitor function detects this number of link changes in the monitored period, then the device performs the specified action.

Possible values:

- 1..100  (default setting: 5)

Last sampling interval

Displays the number of errors that the device has detected during the period that has elapsed.

Total

Displays the total number of errors that the device has detected since the port was enabled.

[CRC/Fragments]

In this tab you specify individually for every port the following settings:

- The detected fragment error rate.
- The period during which the Port Monitor function monitors a parameter to detect discrepancies.

You also see the fragment error rate that the device has detected up to now.

The Port Monitor function monitors those ports for which the checkbox in the CRC/Fragments on column is marked on the Global tab.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.
Sampling interval [s]

Specifies in seconds, the period during which the Port Monitor function monitors a parameter to detect discrepancies.

Possible values:
- 5..180  (default setting: 10)

CRC/Fragments count [ppm]

Specifies the detected fragment error rate (in parts per million).

If the Port Monitor function detects this fragment error rate in the monitored period, then the device performs the specified action.

Possible values:
- 1..1000000  (default setting: 1000)

Last active interval [ppm]

Displays the fragment error rate that the device has detected during the period that has elapsed.

Total [ppm]

Displays the fragment error rate that the device has detected since the port was enabled.

[Overload detection]

In this tab you specify individually for every port the following settings:
- The load threshold values.
- The period during which the Port Monitor function monitors a parameter to detect discrepancies.

You also see the number of data packets that the device has detected up to now.

The Port Monitor function monitors those ports for which the checkbox in the Overload detection on column is marked on the Global tab.

The Port Monitor function does not monitor any ports that are members of a link aggregation group.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.
Traffic type

Specifies the type of data packets that the device takes into account when monitoring the load on the port.

Possible values:
- **all**
  The *Port Monitor* function monitors Broadcast, Multicast and Unicast packets.
- **bc** (default setting)
  The *Port Monitor* function monitors only Broadcast packets.
- **bc-mc**
  The *Port Monitor* function monitors only Broadcast and Multicast packets.

Threshold type

Specifies the unit for the data rate.

Possible values:
- **pps** (default setting)
  packets per second
- **kbps**
  kbit per second
  The prerequisite is that in the Traffic type column the value *all* is specified.

Lower threshold

Specifies the lower threshold value for the data rate.

The *Auto-Disable* function enables the port again only when the load on the port is lower than the value specified here.

Possible values:
- **0..10000000** (default setting: 0)

Upper threshold

Specifies the upper threshold value for the data rate.

If the *Port Monitor* function detects this load in the monitored period, then the device performs the specified action.

Possible values:
- **0..10000000** (default setting: 0)

Interval [s]

Specifies in seconds, the period that the *Port Monitor* function observes a parameter to detect that a parameter is being exceeded.

Possible values:
- **1..20** (default setting: 1)

Packets

Displays the number of Broadcast, Multicast and Unicast packets that the device has detected during the period that has elapsed.
Broadcast packets

Displays the number of Broadcast packets that the device has detected during the period that has elapsed.

Multicast packets

Displays the number of Multicast packets that the device has detected during the period that has elapsed.

Kbit/s

Displays the data rate in Kbits per second that the device has detected during the period that has elapsed.

[Link speed/Duplex mode detection]

In this tab you activate the allowed combinations of speed and duplex mode for each port.

The Port Monitor function monitors those ports for which the checkbox in the Link speed/Duplex mode detection on column is marked on the Global tab.

The Port Monitor function monitors only enabled physical ports.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

10 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

▶ marked
  The port monitor takes into consideration the speed and duplex combination.

▶ unmarked
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the Global tab.
10 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- **marked**: The port monitor takes into consideration the speed and duplex combination.
- **unmarked**: If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the **Global** tab.

100 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- **marked**: The port monitor takes into consideration the speed and duplex combination.
- **unmarked**: If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the **Global** tab.

100 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- **marked**: The port monitor takes into consideration the speed and duplex combination.
- **unmarked**: If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the **Global** tab.

1,000 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.

Possible values:

- **marked**: The port monitor takes into consideration the speed and duplex combination.
- **unmarked**: If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the **Global** tab.
6.5.4 **Auto-Disable**

The **Auto-Disable** function lets you disable monitored ports automatically and enable them again as you desire.

For example, the **Port Monitor** function and selected functions in the **Network Security** menu use the **Auto-Disable** function to disable ports if monitored parameters are exceeded.

If the parameters are no longer being exceeded, then the **Auto-Disable** function enables the relevant port again after the specified waiting period.

The dialog contains the following tabs:
- **[Port]**
- **[Status]**

**[Port]**

This tab displays which ports are currently disabled due to the parameters being exceeded. If the parameters are no longer being exceeded and you specify a waiting period in the **Reset timer [s]** column, then the **Auto-Disable** function automatically enables the relevant port again.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Reset**

Opens the **Which statistic should be deleted?** window. The window displays the ports that you can enable again and reset the related counters to 0. Click and select a table row to enable the corresponding port again.

This affects the counters in the following dialogs:
- **Diagnostics > Ports > Auto-Disable** dialog
- **Diagnostics > Ports > Port Monitor** dialog
  - **Link flap** tab
  - **CRC/Fragments** tab
  - **Overload detection** tab

**Port**

Displays the port number.
**Reset timer [s]**

Specifies the waiting period in seconds, after which the Auto-Disable function enables the port again.

Possible values:
- 0 (default setting)
  The timer is inactive. The port remains disabled.
- 30..4294967295
  If the parameters are no longer being exceeded, then the Auto-Disable function enables the port again after the waiting period specified here.

**Error time**

Displays when the device disabled the port due to the parameters being exceeded.

**Remaining time [s]**

Displays the remaining time in seconds, until the Auto-Disable function enables the port again.

**Component**

Displays the software component in the device that disabled the port.

Possible values:
- PORT_MON
  Port Monitor
  See the Diagnostics > Ports > Port Monitor dialog.
- PORT_ML
  Port Security
  See the Network Security > Port Security dialog.
- DOT1S
  BPDU guard
  See the Switching > L2-Redundancy > Spanning Tree > Global dialog.

**Reason**

Displays the monitored parameter that led to the port being disabled.

Possible values:
- none
  No monitored parameter. The port is enabled.
- link-flap
  Too many link changes. See the Diagnostics > Ports > Port Monitor dialog, Link flap tab.
- crc-error
  Too many CRC/fragment errors are detected. See the Diagnostics > Ports > Port Monitor dialog, CRC/Fragments tab.
- duplex-mismatch
  Duplex mismatch detected. See the Diagnostics > Ports > Port Monitor dialog, Global tab.
- bpdu-rate
  STP-BPDUs received. See the Switching > L2-Redundancy > Spanning Tree > Global dialog.
- mac-based-port-security
  Too many data packets from undesired senders. See the Network Security > Port Security dialog.
- overload-detection
  Overload. See the Diagnostics > Ports > Port Monitor dialog, Overload detection tab.
speed-duplex
Impermissible combination of speed and duplex mode detected. See the Diagnostics > Ports > Port Monitor dialog, Link speed/Duplex mode detection tab.

Loop protection
A layer 2 network loop detected on the port. See the Diagnostics > Loop Protection dialog, Loop detected column.

Active
Displays if the port is currently disabled due to the parameters being exceeded.

Possible values:
- marked
  The port is currently disabled.
- unmarked
  The port is enabled.

[Status]
This tab displays the monitored parameters for which the Auto-Disable function is active.

Table
For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Reason
Displays the parameters that the device monitors.

Mark the adjacent checkbox so that the Auto-Disable function disables and, when applicable, enables the port again if the monitored parameters are exceeded.

Category
Displays which function the adjacent parameter belongs to.

Possible values:
- port-monitor
  The parameter belongs to the functions in the Diagnostics > Ports > Port Monitor dialog.
- network-security
  The parameter belongs to the functions in the Network Security dialog.
- 12-redundancy
  The parameter belongs to the functions in the Switching > L2-Redundancy dialog or to the Loop Protection function, see the Diagnostics > Loop Protection dialog.
Auto-disable

Displays if the Auto-Disable function is active/inactive for the adjacent parameter.

Possible values:

► marked
  The Auto-Disable function for the adjacent parameters is active.
  The Auto-Disable function disables and, when applicable, enables the relevant port again if the monitored parameters are exceeded.

► unmarked (default setting)
  The Auto-Disable function for the adjacent parameters is inactive.
6.5.5 Port Mirroring

The Port Mirroring function lets you copy received and sent data packets from selected ports to a destination port. You can watch and process the data stream using an analyzer or an RMON probe, connected to the destination port. The data packets remain unmodified on the source port.

Note: To enable the access to the device management using the destination port, mark the checkbox Allow management in the Destination port frame before you enable the Port Mirroring function.

Operation

Buttons

- Reset config

Resets the settings in the dialog to the default settings and transfers the changes to the volatile memory of the device (RAM).

Operation

Enables/disables the Port Mirroring function.

Possible values:

- On
  - The Port Mirroring function is enabled.
  - The device copies the data packets from the selected source ports to the destination port.

- Off (default setting)
  - The Port Mirroring function is disabled.

Destination port

Primary port

Specifies the destination port.

Suitable ports are those ports that are not used for the following purposes:

- Source port
- L2 redundancy protocols

Possible values:

- (default setting)
  - No destination port selected.

- <Port number>
  - Number of the destination port. The device copies the data packets from the source ports to this port.

On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.
**Note:** The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards surplus data packets on the destination port.

**Secondary port**

Specifies a second destination port. The prerequisite is that you have specified a primary port.

Possible values:

- *(default setting)*
  - No destination port selected.

- `<Port number>`
  - Number of the destination port. The device copies the data packets from the source ports to this port.

**Allow management**

Activates/deactivates the access to the device management using the destination port.

Possible values:

- **marked**
  - The access to the device management using the destination port is active.
  - The device lets users have access to the device management using the destination port without interrupting the active Port Mirroring session.
  - The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.
  - The VLAN settings on the destination port remain unchanged. The prerequisite for access to the device management using the destination port is that the destination port is not a member of the VLAN of the device management.

- **unmarked** *(default setting)*
  - The access to the device management using the destination port is inactive.
  - The device prohibits the access to the device management using the destination port.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Source port**

Displays the port number.

**Enabled**

Activates/deactivates the copying of the data packets from this source port to the destination port.

Possible values:

- **marked**
  - The copying of the data packets is active.
  - The port is specified as a source port.
Diagnostics

[Diagnoses > LLDP]

- **unmarked** (default setting)
  - The copying of the data packets is inactive.

- **(Grayed-out display)**
  - It is not possible to copy the data packets for this port.
  - Possible causes:
    - The port is already specified as a destination port.
    - The port is a logical port, not a physical port.

**Note:** The device lets you activate every physical port as source port except for the destination port.

### Type

Specifies which data packets the device copies to the destination port.

On the destination port, the device adds a VLAN tag to the data packets that the source port transmits. The destination port transmits unmodified the data packets that the source port receives.

Possible values:

- **none** (default setting)
  - No data packets.

- **tx**
  - Data packets that the source port transmits.

- **rx**
  - Data packets that the source port receives.

- **txrx**
  - Data packets that the source port transmits and receives.

**Note:** With the **txrx** setting the device copies transmitted and received data packets. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively.

---

### 6.6 LLDP

[Diagnoses > LLDP]

The device lets you gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information lets a network management station map the structure of your network.

This menu lets you configure the topology discovery and to display the information received in table form.

The menu contains the following dialogs:

- **LLDP Configuration**
- **LLDP Topology Discovery**
6.6.1 LLDP Configuration

This dialog lets you configure the topology discovery for every port.

**Operation**

Enables/disables the LLDP function.

Possible values:
- **On** (default setting)
  - The LLDP function is enabled.
  - The topology discovery using LLDP is active in the device.
- **Off**
  - The LLDP function is disabled.

**Configuration**

Transmit interval [s]

Specifies the interval in seconds at which the device transmits LLDP data packets.

Possible values:
- **5..32768** (default setting: **30**)

Transmit interval multiplier

Specifies the factor for determining the time-to-live value for the LLDP data packets.

Possible values:
- **2..10** (default setting: **4**)

The time-to-live value coded in the LLDP header results from multiplying this value with the value in the Transmit interval [s] field.

Reinit delay [s]

Specifies the delay in seconds for the reinitialization of a port.

Possible values:
- **1..10** (default setting: **2**)

If in the Operation column the value **Off** is specified, then the device tries to reinitialize the port after the time specified here has elapsed.
Transmit delay [s]

Specifies the delay in seconds for transmitting successive LLDP data packets after configuration changes in the device occur.

Possible values:
- 1..8192 (default setting: 2)

The recommended value is between a minimum of 1 and a maximum of a quarter of the value in the Transmit interval [s] field.

Notification interval [s]

Specifies the interval in seconds for transmitting LLDP notifications.

Possible values:
- 5..3600 (default setting: 5)

After transmitting a notification trap, the device waits for a minimum of the time specified here before transmitting the next notification trap.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Operation

Specifies if the port transmits and receives LLDP data packets.

Possible values:
- transmit
  The port transmits LLDP data packets but does not save any information about neighboring devices.
- receive
  The port receives LLDP data packets but does not transmit any information to neighboring devices.
- receive and transmit (default setting)
  The port transmits LLDP data packets and saves information about neighboring devices.
- disabled
  The port does not transmit LLDP data packets and does not save information about neighboring devices.
Diagnostics
[Diagnoses > LLDP > Configuration]

Notification

Activates/deactivates the LLDP notifications on the port.

Possible values:

- marked
  LLDP notifications are active on the port.
- unmarked (default setting)
  LLDP notifications are inactive on the port.

Transmit port description

Activates/deactivates the transmitting of a TLV (Type Length Value) with the port description.

Possible values:

- marked (default setting)
  The transmitting of the TLV is active.
  The device transmits the TLV with the port description.
- unmarked
  The transmitting of the TLV is inactive.
  The device does not transmit a TLV with the port description.

Transmit system name

Activates/deactivates the transmitting of a TLV (Type Length Value) with the device name.

Possible values:

- marked (default setting)
  The transmitting of the TLV is active.
  The device transmits the TLV with the device name.
- unmarked
  The transmitting of the TLV is inactive.
  The device does not transmit a TLV with the device name.

Transmit system description

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system description.

Possible values:

- marked (default setting)
  The transmitting of the TLV is active.
  The device transmits the TLV with the system description.
- unmarked
  The transmitting of the TLV is inactive.
  The device does not transmit a TLV with the system description.
Transmit system capabilities

Activates/deactivates the transmitting of the TLV (Type Length Value) with the system capabilities.

Possible values:

- **marked** (default setting)
  The transmitting of the TLV is active.
  The device transmits the TLV with the system capabilities.

- **unmarked**
  The transmitting of the TLV is inactive.
  The device does not transmit a TLV with the system capabilities.

Neighbors (max.)

Limits the number of neighboring devices to be recorded for this port.

Possible values:

- **1..50** (default setting: 10)

FDB mode

Specifies which function the device uses to record neighboring devices on this port.

Possible values:

- **lldpOnly**
  The device uses only LLDP data packets to record neighboring devices on this port.

- **macOnly**
  The device uses learned MAC addresses to record neighboring devices on this port. The device uses the MAC address only if there is no other entry in the address table (FDB, Forwarding Database) for this port.

- **both**
  The device uses LLDP data packets and learned MAC addresses to record neighboring devices on this port.

- **autoDetect** (default setting)
  If the device receives LLDP data packets at this port, then the device operates the same as with the **lldpOnly** setting. Otherwise, the device operates the same as with the **macOnly** setting.
6.6.2 LLDP Topology Discovery

Devices in networks send notifications in the form of packets which are also known as "LLDPDU" (LLDP data units). The data that is sent and received through LLDPDUs is useful for many reasons. Thus the device detects which devices in the network are neighbors and through which ports they are connected.

The dialog lets you display the network and to detect the connected devices along with their specific features.

The dialog contains the following tabs:
- [LLDP]
- [LLDP-MED]

[LLDP]

This tab displays the collected LLDP information for the neighboring devices. This information lets a network management station map the structure of your network.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When only devices without active topology discovery are connected to a port, the table contains one line for this port to represent every device. This line contains the number of connected devices.

The Forwarding Database (FDB) address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

When you use one port to connect several devices, for example through a hub, the table shows one line for each connected device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Neighbor identifier

Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.
**FDB**

Displays if the connected device has active LLDP support.

Possible values:

- **marked**
  - The connected device does not have active LLDP support.
  - The device uses information from its address table (FDB, Forwarding Database)

- **unmarked**
  - The connected device has active LLDP support.

**Neighbor address**

Displays the IPv4 address or hostname with which the access to the neighboring device management is possible.

**Neighbor IPv6 address**

Displays the IPv6 address with which the access to the neighboring device management is possible.

**Neighbor port description**

Displays a description for the port of the neighboring device.

**Neighbor system name**

Displays the device name of the neighboring device.

**Neighbor system description**

Displays a description for the neighboring device.

**Port ID**

Displays the ID of the port through which the neighboring device is connected to the device.

**Autonegotiation supported**

Displays if the port of the neighboring device supports autonegotiation.

**Autonegotiation**

Displays if autonegotiation is active on the port of the neighboring device.

**PoE supported**

Displays if the port of the neighboring device supports Power over Ethernet (PoE).

**PoE enabled**

Displays if Power over Ethernet (PoE) is active on the port of the neighboring device.
LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices and network devices. It specifically provides support for VoIP applications. In this support rule, it provides an additional set of common advertisement, Type Length Value (TLV), messages. The device uses the TLVs for capabilities discovery such as network policy, Power over Ethernet, inventory management and location information.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Device class

Displays the device class of the remotely connected device.

▶ A value of notDefined indicates that the device has capabilities not covered by any of the LLDP-MED classes.

▶ A value of endpointClass1..3 indicates that the device has "endpoint class 1..3" capabilities.

▶ A value of networkConnectivity indicates that the device has network connectivity device capabilities.

VLAN ID

Displays the extension of the VLAN Identifier for the remote system connected to this port, as defined in IEEE 802.3.

▶ The device uses a value from 1 through 4042 to specify a valid Port VLAN ID.

▶ The device displays the value 0 for priority tagged packets. This means that only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port.

Priority

Displays the value of the 802.1D Priority which is associated with the remote system connected to the port.

DSCP

Displays the value of the Differentiated Service Code Point (DSCP) which is associated with the remote system connected to the port.

Unknown bit status

Displays the Unknown Bit Status of incoming data packets.

▶ A value of true indicates that the network policy for the specified application type is currently unknown. In this case, the VLAN ID ignores the Layer 2 priority and value of the DSCP field.

▶ A value of false indicates a specified network policy.
6.7 Loop Protection

The Loop Protection function helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, a poorly connected cable or an incorrect setting in the device.
For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:

- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

In redundant network topologies, multiple redundancy protocols are typically active. You usually disable the Spanning Tree function on the ports involved in other redundancy protocols. The redundancy protocols already help to avoid loops.

### Operation

Enables/disables the Loop Protection function.

Possible values:

- **On**
  - The Loop Protection function is enabled.
  - On active and passive ports, the device evaluates received loop detection packets.
  - On active ports, the device sends loop detection packets at regular intervals as specified in the Transmit interval field.
  - The prerequisite is that the Loop Protection function is active on the port.
  - The device lets you monitor Ethernet loops with the signal contact. See the Diagnostics > Status Configuration > Signal Contact > Signal Contact 1 dialog, checkbox for the Ethernet loops parameter.

- **Off** (default setting)
  - The Loop Protection function is disabled.
  - The device neither sends loop detection packets nor evaluates received loop detection packets.

### Configuration

Activates/deactivates the Auto-Disable function for Loop Protection.

Possible values:

- **marked**
  - The Auto-Disable function for Loop Protection is active.
  - The prerequisite for disabling the port is that in the Action column the value auto-disable or all is specified.
  - The device lets you specify the waiting period in seconds after which the Auto-Disable function enables the port again. To do this, in the Diagnostics > Ports > Auto-Disable dialog, specify the waiting period in the Reset timer [s] column.

- **unmarked** (default setting)
  - The Auto-Disable function for Loop Protection is inactive.
Global

Transmit interval

Specifies the interval in seconds at which the device sends loop detection packets if the Loop Protection function is active on the port.

Possible values:
▶ 1..10

Receive threshold

Specifies the threshold value for the number of loop detection packets received in a row. If the number reaches or exceeds this threshold, then the device will perform the action specified in the Action column.

Possible values:
▶ 1..50

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Clear port statistics

Resets the values in the following columns:

• Loop count
• Sent frames
• Received frames

Port

Displays the port number.

Active

Activates/deactivates the Loop Protection function on the port.

Possible values:
▶ marked
  The Loop Protection function is active on the port.
  Activate the function only on ports which are not part of a redundant network path. This helps avoid an accidental shutdown of redundant network paths.
  If the device receives a loop detection packet on this port, sent from another port on the same device, then the device performs the action specified in the Action column.
▶ unmarked (default setting)
  The Loop Protection function is inactive on the port. The port neither sends loop detection packets nor evaluates received loop detection packets.
Mode

Specifies the behavior of the Loop Protection function on the port.

Possible values:
- active
  The device sends loop detection packets and evaluates received loop detection packets.
- passive (default setting)
  The device evaluates received loop detection packets.

Action

Specifies the action the device performs when it detects a layer 2 network loop on this port.

Possible values:
- trap
  The device sends a trap.
- auto-disable (default setting)
  The device disables the port using the Auto-Disable function.
  The prerequisite for disabling the port is that in the Configuration frame the Auto-disable checkbox is marked.
- all
  The device sends a trap. Then the device disables the port using the Auto-Disable function.
  The prerequisite for disabling the port is that in the Configuration frame the Auto-disable checkbox is marked.

VLAN ID

Specifies the VLAN in which the device sends the loop detection packets.

Possible values:
- 0 (default setting)
  The device sends the loop detection packets without a VLAN tag.
- 1..4042
  The device sends the loop detection packets in the specified VLAN. The prerequisite is that in the Switching > VLAN > Port dialog the VLAN is already set up and that the port is a member of the VLAN.

Loop detected

Displays if the device has detected a layer 2 network loop on the port.

Possible values:
- yes
  The device has detected a layer 2 network loop on the port.
  After the loop has ended and the port is enabled again, the device resets the value to no.
- no
  The device has not detected a layer 2 network loop on the port.

Loop count

Displays the number of loops the device has detected on the port since the last port statistics reset or since the last system startup.
Last loop time

Displays the time at which the device detected the last loop on the port.

The prerequisite for the correct evaluation of the value is that in the Time > Basic Settings dialog the system time of the device is synchronized with the appropriate reference time.

Sent frames

Displays the number of loop detection packets sent on the port since the last port statistics reset or since the last system startup.

Received frames

Displays the number of sent and received back loop detection packets on the port since the last port statistics reset or since the last system startup.

Discarded frames

Displays the number of discarded loop detection packets on the port.

Examples of reasons for discarded packets:

- The device detects packets with an incorrect format.
- The device detects packets with expired timestamps (packets received more than 5 seconds after sending).
- The device received a data packet with an unexpected VLAN information.
- The device detects received packets on a port that is disabled.
6.8 Report

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail
6.8.1 Report Global

The device lets you log specific events using the following outputs:

- on the console
- on one or more syslog servers
- on a connection to the Command Line Interface set up using SSH
- on a connection to the Command Line Interface set up using Telnet

In this dialog you specify the required settings. By assigning the severity you specify which events the device registers.

The dialog lets you save a ZIP archive with detailed device information for support purposes on your PC.

**Console logging**

**Buttons**

- Download support information
  
  Generates a ZIP archive which the web browser lets you download from the device.

  The ZIP archive contains files with detailed device information for support purposes. For further information, see “Support Information: Files in ZIP archive” on page 342.

**Operation**

Enables/disables the *Console logging* function.

Possible values:

- **On**
  
  The *Console logging* function is enabled.
  
  The device logs the events on the console.

- **Off** (default setting)
  
  The *Console logging* function is disabled.

**Severity**

Specifies the minimum severity for the events. The device logs events with this severity and with more urgent severities. For further information, see “Meaning of the event severities” on page 342.

The device outputs the messages on the serial interface.

Possible values:

- emergency
- alert
- critical
- error
- warning (default setting)
- notice
SNMP logging

When you enable the logging of SNMP requests, the device sends these as events with the preset severity notice to the list of syslog servers. The preset minimum severity for a syslog server entry is critical.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- Set the severity for which the device creates SNMP requests as events to warning or error. Change the minimum severity for a syslog entry for one or more syslog servers to the same value.
  - You also have the option of creating a separate syslog server entry for this.
- Set only the severity for SNMP requests to critical or higher. The device then sends SNMP requests as events with the severity critical or higher to the syslog servers.
- Set only the minimum severity for one or more syslog server entries to notice or lower. Then it is possible that the device sends many events to the syslog servers.

Log SNMP get request

Enables/disables the logging of SNMP Get requests.

Possible values:

- On
  - The logging is enabled.
  - The device registers SNMP Get requests as events in the syslog.
  - From the Severity get request drop-down list, you select the severity for this event.
- Off (default setting)
  - The logging is disabled.

Log SNMP set request

Enables/disables the logging of SNMP Set requests.

Possible values:

- On
  - The logging is enabled.
  - The device registers SNMP Set requests as events in the syslog.
  - From the Severity set request drop-down list, you select the severity for this event.
- Off (default setting)
  - The logging is disabled.

Severity get request

Specifies the severity of the event that the device registers for SNMP Get requests. For further information, see “Meaning of the event severities” on page 342.

Possible values:

- emergency
- alert
- critical
Severity set request

Specifies the severity of the event that the device registers for SNMP Set requests. For further information, see “Meaning of the event severities” on page 342.

Possible values:
- emergency
- alert
- critical
- error
- warning
- notice (default setting)
- informational
- debug

Buffered logging

The device buffers logged events in 2 separate storage areas so that the log entries for urgent events are kept.

This dialog lets you specify the minimum severity for events that the device buffers in the storage area with a higher priority.

Severity

Specifies the minimum severity for the events. The device buffers log entries for events with this severity and with more urgent severities in the storage area with a higher priority. For further information, see “Meaning of the event severities” on page 342.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug
**CLI logging**

**Operation**

Enables/disables the *CLI logging* function.

Possible values:

- **On**
  - The *CLI logging* function is enabled.
  - The device logs every command received using the Command Line Interface.

- **Off** (default setting)
  - The *CLI logging* function is disabled.

**Support Information: Files in ZIP archive**

<table>
<thead>
<tr>
<th>File name</th>
<th>Format</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>audittrail.html</td>
<td>HTML</td>
<td>Contains the chronological recording of the system events and saved user changes in the Audit Trail.</td>
</tr>
<tr>
<td>config.xml</td>
<td>XML</td>
<td>Contains the settings of the device saved in the &quot;Selected&quot; configuration profile.</td>
</tr>
<tr>
<td>defaultconfig.xml</td>
<td>XML</td>
<td>Contains the default settings of the device.</td>
</tr>
<tr>
<td>script</td>
<td>TEXT</td>
<td>Contains the output of the command <code>show running-config script</code>.</td>
</tr>
<tr>
<td>runningconfig.xml</td>
<td>XML</td>
<td>Contains the current operating settings of the device.</td>
</tr>
<tr>
<td>supportinfo.html</td>
<td>TEXT</td>
<td>Contains device internal service information.</td>
</tr>
<tr>
<td>systeminfo.html</td>
<td>HTML</td>
<td>Contains information about the current settings and operating parameters.</td>
</tr>
<tr>
<td>systemlog.html</td>
<td>HTML</td>
<td>Contains the logged events in the Log file. See the <em>Diagnostics &gt; Report &gt; System Log</em> dialog.</td>
</tr>
</tbody>
</table>

**Meaning of the event severities**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>Device not ready for operation</td>
</tr>
<tr>
<td>alert</td>
<td>Immediate user intervention required</td>
</tr>
<tr>
<td>critical</td>
<td>Critical status</td>
</tr>
<tr>
<td>error</td>
<td>Error status</td>
</tr>
<tr>
<td>warning</td>
<td>Warning</td>
</tr>
<tr>
<td>notice</td>
<td>Significant, normal status</td>
</tr>
<tr>
<td>informational</td>
<td>Informal message</td>
</tr>
<tr>
<td>debug</td>
<td>Debug message</td>
</tr>
</tbody>
</table>
6.8.2 **Persistent Logging**

The device lets you save log entries permanently in a file in the external memory. Therefore, even after the device is restarted you have access to the log entries.

In this dialog you limit the size of the log file and specify the minimum severity for the events to be saved. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly created file.

In the table the device displays you the log files held in the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space in the external memory.

**Note:** Verify that an external memory is connected. To verify if an external memory is connected, see the **Status** column in the **Basic Settings > External Memory** dialog. We recommend to monitor the external memory connection using the **Device Status** function, see the **External memory removal** parameter in the **Diagnostics > Status Configuration > Device Status** dialog.

**Operation**

Enables/disables the **Persistent Logging** function.

Only activate this function if the external memory is available in the device.

Possible values:

- **On** (default setting)
  - The **Persistent Logging** function is enabled.
  - The device saves the log entries in a file in the external memory.

- **Off**
  - The **Persistent Logging** function is disabled.

**Configuration**

**Max. file size [kbyte]**

Specifies the maximum size of the log file in KBytes. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly created file.

Possible values:

- **0..4096** (default setting: 1024)
  - The value 0 deactivates saving of log entries in the log file.
Files (max.)

Specifies the number of log files that the device keeps in the external memory.

As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files.

Possible values:
- 0..25 (default setting: 4)

The value 0 deactivates saving of log entries in the log file.

Severity

Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory.

Possible values:
- emergency
- alert
- critical
- error
- warning (default setting)
- notice
- informational
- debug

Log file target

Specifies the external memory device for logging.

Possible values:
- usb
  External USB memory (ACA21/ACA22)

Table

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

Buttons

Delete persistent log file

Removes the log files from the external memory.
Index
Displays the index number to which the table row relates.
Possible values:
► 1..25
The device automatically assigns this number.

File name
Displays the file name of the log file in the external memory.
Possible values:
► messages
► messages.X

File size [byte]
Displays the size of the log file in the external memory in bytes.
6.8.3 System Log

The device logs device-internal events in a log file (System Log).

This dialog displays the log file (System Log). The dialog lets you save the log file in HTML format on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The log file is kept until a restart is performed in the device. After the restart the device creates the file again.

Buttons

Save log file

Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.

Delete log file

Removes the logged events from the log file.
6.8.4 **Audit Trail**

This dialog displays the log file (Audit Trail). The dialog lets you save the log file as an HTML file on your PC.

In order to search the log file for search terms, use the search function of your web browser.

The device logs system events and writing user actions in the device. This lets you keep track of WHO changes WHAT in the device and WHEN. The prerequisite is that the access role **auditor** or **administrator** is assigned to your user account.

The device logs the following user actions, among others:
- A user logging in with the Command Line Interface (local or remote)
- A user logging off manually
- Automatic logging off of a user in the Command Line Interface after a specified period of inactivity
- Device restart
- Locking of a user account due to too many unsuccessful login attempts
- Locking of the access to the device management due to unsuccessful login attempts
- Commands executed in the Command Line Interface, apart from `show commands`
- Changes to configuration variables
- Changes to the system time
- File transfer operations, including firmware updates
- Configuration changes using HiDiscovery
- Firmware updates and automatic configuration of the device through the external memory
- Opening and closing of SNMP through an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

**Note:** During the system startup, access to the system monitor is possible using the default settings of the device. If an attacker gains physical access to the device, then he is able to reset the device settings to its default values using the system monitor. After this, the device and log file are accessible using the standard password. Take appropriate measures to restrict physical access to the device. Otherwise, deactivate access to the system monitor. See the **Diagnostics > System > Selftest** dialog, **SysMon1 is available** checkbox.

**Buttons**

- **Save audit trail file**

  Opens the HTML page in a new web browser window or tab. You can save the HTML page on your PC using the appropriate web browser command.
7 Advanced

The menu contains the following dialogs:
- DHCP L2 Relay
- DHCP Server
- DNS
- Industrial Protocols
- Command Line Interface

7.1 DHCP L2 Relay

A network administrator uses the DHCP L2 Relay Agent to add DHCP client information. L3 Relay Agents and DHCP servers need the DHCP client information to assign an IP address and a configuration to the clients.

When active, the relay adds Option 82 information configured in this dialog to the packets before it relays DHCP requests from the clients to the server. The Option 82 fields provide unique information about the client and relay. This unique identifier consists of a Circuit ID for the client and a Remote ID for the relay.

In addition to the type, length, and multicast fields, the Circuit ID includes the VLAN ID, unit number, slot number, and port number for the connected client.

The Remote ID consists of a type and length field and either a MAC address, IP address, client identifier, or a user-defined device description. A client identifier is the user-defined system name for the device.

For the DHCPv6 protocol, the device uses a Relay Agent to add Relay Agent options to DHCPv6 packets exchanged between a client and a DHCPv6 server. The Lightweight DHCPv6 Relay Agent (LDRA) is described in RFC 6221.

The LDRA processes 2 types of messages:
- Relay-Forward messages
  The Relay Agent forwards Relay-Forward messages that contain unique information about the client. The client information includes the peer-address, meaning the IPv6 link-local address of the client and the Interface-ID information. The Interface-ID information, also known as Option 18, provides information that identifies the interface on which the client request was sent.
- Relay-Reply messages
  The DHCPv6 server sends Relay-Reply messages. The Relay Agent validates the messages to include the information encapsulated in the initial Relay-Forward message. If the information is valid, then the Relay Agent forwards the packet to the client.

The menu contains the following dialogs:
- DHCP L2 Relay Configuration
- DHCP L2 Relay Statistics
7.1.1 DHCP L2 Relay Configuration

This dialog lets you activate the relay function on an interface and VLAN. When you activate this function on a port, the device either relays the Option 82 information or drops the information on untrusted ports. Furthermore, the device lets you specify the remote identifier.

The Option 82 information is specific to DHCPv4 L2 Relay function. For DHCPv6 L2 Relay function, the Option 18 information is used in the packet exchange between the client and DHCPv6 server. The device discards DHCPv6 packets received on ports that do not contain Option 18 information.

The dialog contains the following tabs:
- [Interface]
- [VLAN ID]

Operation

Enables/disables the DHCP L2 Relay function of the device globally.

With this function enabled, DHCPv4 L2 Relay and DHCPv6 L2 Relay functions can operate at the same time in the device.

Possible values:
- **On**
  Enables the DHCP L2 Relay function in the device.
- **Off** (default setting)
  Disables the DHCP L2 Relay function in the device.

[Interface]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Port

Displays the port number.

Active

Activates/deactivates the DHCP L2 Relay function on the port.

The prerequisite is that you enable the function globally.
Possible values:

- marked
  The **DHCP L2 Relay** function is active.
- unmarked (default setting)
  The **DHCP L2 Relay** function is inactive.

**Trusted port**

Activates/deactivates the secure **DHCP L2 Relay** mode for the corresponding port.

Possible values:

- marked
  The device accepts DHCPv4 packets with *Option 82* information. The device accepts DHCPv6 packets with *Option 18* information.
- unmarked (default setting)
  The device discards DHCPv4 packets received on non-secure ports that contain *Option 82* information. The device discards DHCPv6 packets received on ports that do not contain *Option 18* information.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**VLAN ID**

VLAN to which the table row relates.

**Active**

Activates/deactivates the **DHCP L2 Relay** function on the VLAN.

The prerequisite is that you enable the function globally.

Possible values:

- marked
  The **DHCP L2 Relay** function is active.
- unmarked (default setting)
  The **DHCP L2 Relay** function is inactive.
Circuit ID

Activates or deactivates the addition of the Circuit ID to the Option 82 information.

Possible values:
- **marked** (default setting)
  - Enables Circuit ID and Remote ID to be sent together.
- **unmarked**
  - The device sends only the Remote ID.

Remote ID type

Specifies the components of the Remote ID for this VLAN. The Remote ID field displays the string the device uses as Remote ID.

Possible values:
- **ip**
  - Specifies the IP address of the device as Remote ID.
- **mac** (default setting)
  - Specifies the MAC address of the device as Remote ID.
- **client-id**
  - Specifies the system name of the device as Remote ID.
- **other**
  - When you select this item, enter any character string in the Remote ID column.

Remote ID

Displays the Remote ID that the device uses for this VLAN. If the item **other** is selected from the Remote ID type drop-down list, then enter any character string.

Possible values:
- Alphanumeric ASCII character string with 1..32 characters

The device enters ASCII code values into the packet. If the item **client-id** or **other** is selected from the Remote ID type drop-down list, then the device processes the ASCII code of the characters. For example, when you enter the string **abc**, the device enters the value **616263** into the packet.

If the device does not accept the string you entered, then perform the following steps:
- Click the button to undo the unsaved changes in the current dialog.
- From the Remote ID type drop-down list, select the item **other**.
- Click the button without modifying the string.
- Enter the arbitrary string.
7.1.2 DHCP L2 Relay Statistics

The device monitors the data stream on the ports and displays the results in tabular form. This table is divided into various categories to aid you in data stream analysis. The DHCPv6 relay options are not displayed in the statistics table.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

Reset

Resets the counter for the statistics to 0.

Port

Displays the port number.

Untrusted server messages with Option 82

Displays the number of DHCP server messages received with Option 82 information on the untrusted interface.

Untrusted client messages with Option 82

Displays the number of DHCP client messages received with Option 82 information on the untrusted interface.

Trusted server messages without Option 82

Displays the number of DHCP server messages received without Option 82 information on the trusted interface.

Trusted client messages without Option 82

Displays the number of DHCP client messages received without Option 82 information on the trusted interface.
7.2 DHCP Server

With the DHCP server, you manage a database of available IP addresses and configuration information. When the device receives a request from a client, the DHCP server validates the DHCP client network, and then leases an IP address. When enabled, the DHCP server also allocates configuration information appropriate for that client. The configuration information specifies, for example, which IP address, DNS server and the default route a client uses.

The DHCP server assigns an IP address to a client for a user-defined interval. The DHCP client is responsible for renewing the IP address before the interval expires. When the DHCP client is unable to renew the address, the address returns to the pool for reassignment.

The menu contains the following dialogs:
- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table
7.2.1 DHCP Server Global

Activate the function either globally or per port according to your requirements.

**Operation**

Enables/disables the DHCP server function of the device globally.

Possible values:
- **On**
- **Off** (default setting)

**Configuration**

Activates/deactivates the probing for unique IP addresses. Before assigning an IP address, the server uses an *ICMP Echo* request to check whether this IP address is already in use on the network.

Possible values:
- **marked** (default setting)
  - The *IP Probe* function is active.
- **unmarked**
  - The *IP Probe* function is inactive.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Port**

Displays the port number.

**DHCP server active**

Activates/deactivates the DHCP server function on this port.

The prerequisite is that you enable the function globally.
Possible values:

- **marked** (default setting)
  The DHCP server function is active.
- **unmarked**
  The DHCP server function is inactive.
7.2.2 DHCP Server Pool

In this dialog, you specify the settings for assigning a specific IP address to DHCP clients from which the device receives a DHCP request. Depending on if a requesting device is connected to a physical port or is a member of a VLAN, the DHCP server assigns an IP address from a specific pool (address range).

The device provides a maximum of 128 pools, in total a maximum of 1000 entries. The DHCP server offers the following IP address allocation modes:

- **Static**
  The device assigns a static entry based on a pool containing 1 IP address (IP address = last IP address). This is useful to assign the same IP address to a specific device, for example, a server, NAS, or printer. The device assigns the address based on:
  - The MAC address of the client
  - The physical port, to which the client is connected
  - The VLAN of which the client is a member

- **Dynamic**
  The device assigns a dynamic entry based on a pool containing more than 1 IP address. This is useful to assign an IP address from a particular address range, for example, to clients that are a member of a particular VLAN.

If desired, the device also processes further information from the DHCP request to assign an IP address from a specific pool to the client. This further information can be, for example, a client ID, a remote ID, or a circuit ID.

You can specify individual parameters (DHCP options) for each pool. The device sends these parameters to the clients together with the IP address. Supplying DHCP options is a smart way to set up network clients during the early phase of network access deployment.

This dialog displays different information that is required for the assignment of an IP address to a client on a port or in a VLAN. Use the button to add a table row.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  Adds a table row.

- **Remove**
  Removes the selected table row.

**Index**

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.
Advanced
[Advanced > DHCP Server > Pool]

Active

Activates/deactivates the DHCP server function on this port.

Possible values:
- marked
  - The DHCP server function is active.
- unmarked (default setting)
  - The DHCP server function is inactive.

IP address

Specifies the IP address for static IP address assignment. When using dynamic IP address assignment, this value specifies the start of the IP address range.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Last IP address

When using dynamic IP address assignment, this value specifies the end of the IP address range.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

Port

Specifies the port number.

Possible values:
- All (default setting)
  - The device assigns an IP address to a client device regardless of the port on which the local device receives the DHCP request.
- <Port number>
  - The device assigns an IP address to a client device only if the local device receives the DHCP request on the specified port.

VLAN ID

Specifies the VLAN to which the table row relates.

A value of 1 corresponds to the default device management VLAN.

Possible values:
- (default setting)
- 1..4042

MAC address

 Specifies the MAC address of the device leasing the IP address.

Possible values:
- (default setting)
  - For the IP address assignment, the server ignores this variable.
- Valid Unicast MAC address
  - Specify the value with a colon separator, for example 00:11:22:33:44:55.
DHCP relay

Specifies the IP address of the DHCP relay through which the clients transmit their requests to the DHCP server. When the DHCP server receives a client’s request through another DHCP relay, it ignores this request.

Possible values:
- (default setting)
  No DHCP relay specified.
- Valid IPv4 address
  IP address of the DHCP relay.

Client ID

Specifies the customized identifier for the client instead of the MAC address.

Possible values:
- (default setting)
  The device ignores the parameter during assignment of an IP address from the pool.
- Sequence of hexadecimal character pairs with 1..254 pairs separated by a space.
  Example: 41 42 43 44 4F

Note: If you have high security requirements and do not want to trust the clients implicitly, consider using the remote ID or the circuit ID instead of the client ID. The remote ID and the circuit ID are inserted by a DHCP relay and are therefore harder to spoof.

Remote ID

Specifies the remote ID. The DHCP relay inserts the remote ID into the DHCP request.

Possible values:
- (default setting)
  The device ignores the parameter during assignment of an IP address from the pool.
- Sequence of hexadecimal character pairs with 1..254 pairs separated by a space.
  Example: 41 42 43 44 4F

Circuit ID

Specifies the circuit ID. The DHCP relay inserts the circuit ID into the DHCP request.

Possible values:
- (default setting)
  The device ignores the parameter during assignment of an IP address from the pool.
- Sequence of hexadecimal character pairs with 1..254 pairs separated by a space.
  Example: 41 42 43 44 4F
Hirschmann device

Activates/deactivates the Hirschmann multicasts. If the device in this IP address range serves only the Hirschmann clients, then activate this function.

Possible values:
- **marked**  
  In this IP address range, the device serves only the Hirschmann clients. The Hirschmann multicasts are activated.
- **unmarked**  
  (default setting)  
  In this IP address range, the device serves the clients of different manufacturers. The Hirschmann multicasts are deactivated.

Configuration URL

Specifies the protocol to be used as well as the name and path of the configuration file.

Possible values:
- Alphanumeric ASCII character string with 0..70 characters  
  Example: tftp://192.9.200.1/cfg/config.xml

When you leave this field blank, the device leaves this option field blank in the DHCP message.

Lease time [s]

Specifies the lease time in seconds.

Possible values:
- 60..220752000  
  (default setting: 86400)
- 4294967295  
  Use this value for assignments unlimited in time and for assignments using BOOTP.

Default gateway

Specifies the IP address of the default gateway.

A value of 0.0.0.0 disables the attachment of the option field in the DHCP message.

Possible values:
- Valid IPv4 address  
  (default setting: 0.0.0.0)

Netmask

Specifies the mask of the network to which the client belongs.

A value of 0.0.0.0 disables the attachment of the option field in the DHCP message.

Possible values:
- Valid IPv4 netmask  
  (default setting: 255.255.255.0)

WINS server

Specifies the IP address of the Windows Internet Name Server which converts NetBIOS names.

A value of 0.0.0.0 disables the attachment of the option field in the DHCP message.
Possible values:
▶ Valid IPv4 address (default setting: 0.0.0.0)

DNS server

Specifies the IP address of the DNS server.

A value of 0.0.0.0 disables the attachment of the option field in the DHCP message.

Possible values:
▶ Valid IPv4 address (default setting: 0.0.0.0)

Hostname

Specifies the hostname.

When you leave this field blank, the device leaves this option field blank in the DHCP message.

Possible values:
▶ Alphanumeric ASCII character string with 0..64 characters
### 7.2.3 DHCP Server Lease Table

This dialog displays the status of IP address leasing on a per port basis.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the port number to which the address is currently being leased.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Displays the leased IP address to which the entry refers.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the lease phase.</td>
</tr>
</tbody>
</table>

According to the standard for DHCP operations, there are 4 phases to leasing an IP address: Discovery, Offer, Request, and Acknowledgement.

Possible values:

- **bootp**
  A DHCP client is attempting to discover a DHCP server for IP address allocation.
- **offering**
  The DHCP server is validating that the IP address is suitable for the client.
- **requesting**
  A DHCP client is acquiring the offered IP address.
- **bound**
  The DHCP server is leasing the IP address to a client.
- **renewing**
  The DHCP client is requesting an extension to the lease.
- **rebinding**
  The DHCP server is assigning the IP address to the client after a successful renewal.
- **declined**
  The DHCP server denied the request for the IP address.
- **released**
  The IP address is available for other clients.

| Remaining lifetime | Displays the time remaining on the leased IP address. |

| Leased MAC address | Displays the MAC address of the device leasing the IP address. |
Gateways

Displays the Gateway IP address of the device leasing the IP address.

Client ID

Displays the client ID of the device leasing the IP address.

Remote ID

Displays the remote ID of the device leasing the IP address.

Circuit ID

Displays the circuit ID of the device leasing the IP address.

7.3 DNS

[Advanced > DNS]

The menu contains the following dialogs:

► DNS Client

7.3.1 DNS Client

[Advanced > DNS > Client]

DNS (Domain Name System) is a service in the network that translates host names into IP addresses. This name resolution lets you contact other devices using their host names instead of their IP addresses.

Using the Client function the device sends requests for resolving hostnames in IP addresses to a DNS server.

The menu contains the following dialogs:

► DNS Client Global
► DNS Client Current
► DNS Client Static
► DNS Client Static Hosts
7.3.1.1 DNS Client Global

In this dialog you enable the Client function and the Cache function.

Operation

Enables/disables the Client function.

Possible values:

- **On**
  - The Client function is enabled.
  - The device sends requests for resolving hostnames in IP addresses to a DNS server.

- **Off** (default setting)
  - The Client function is disabled.

Cache

Enables/disables the Cache function.

Possible values:

- **On** (default setting)
  - The Cache function is enabled.
  - The device temporarily saves up to 128 DNS server responses (hostname and corresponding IP address) in the cache. When the cache contains a matching entry, the host name of a new request the device resolves itself. This makes sending a new query to the DNS server unnecessary.

- **Off**
  - The Cache function is disabled.
7.3.1.2 DNS Client Current

This dialog displays to which DNS servers the device sends requests for resolving hostnames in IP addresses.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Index**

Displays the sequential number of the DNS server.

**Address**

Displays the IP address of the DNS server. The device forwards requests for resolving hostnames in IP addresses to the DNS server with this IP address.
7.3.1.3 DNS Client Static

In this dialog you specify the DNS servers to which the device forwards requests for resolving host names in IP addresses.

The device lets you specify up to 4 IP addresses yourself or to transfer the IP addresses from a DHCP server.

Configuration

Configuration source

Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests.

Possible values:

► user
  The device uses the IP addresses specified in the table.

► mgmt-dhcp (default setting)
  The device uses the IP addresses which the DHCP server delivers to the device.

Domain name

Specifies the domain name according to RFC1034 which the device adds to hostnames without a domain suffix.

Possible values:

► Alphanumeric ASCII character string with 0..255 characters

Request timeout [s]

Specifies the time interval in seconds for sending again a request to the server.

Possible values:

► 0
  Deactivates the function. The device does not send a request to the server again.

► 1..3600 (default setting: 3)

Request retransmits

Specifies, how many times the device retransmits a request.

The prerequisite is that in the Request timeout [s] field a value > 0 is specified.
Possible values:

- 0..100 (default setting: 2)

**Table**

For information on how to customize the appearance of the table, see "Working with tables" on page 16.

**Buttons**

- Add
  Adds a table row.

- Remove
  Removes the selected table row.

**Index**

Displays the sequential number of the DNS server. The device automatically assigns the value when you add a table row.

The device lets you specify up to 4 DNS servers.

**Address**

Specifies the IP address of the DNS server.

Possible values:

- Valid IPv4 address (default setting: 0.0.0.0)
- Valid IPv6 address

**Active**

Activates/deactivates the table row.

The device sends requests to the DNS server configured in the first active table row. When the device does not receive a response from this server, it sends requests to the DNS server configured in the next active table row.

Possible values:

- marked
  The DNS client sends requests to this DNS server.

  Prerequisites:
  - In the Advanced > DNS > Client > Global dialog the DNS-client function is enabled.
  - In the Configuration frame, Configuration source drop-down list the item user is selected.

- unmarked (default setting)
  The device does not send requests to this DNS server.
7.3.1.4 DNS Client Static Hosts

This dialog lets you specify up to 64 hostnames which you link with one IP address each. Upon a request for resolving hostnames in IP addresses, the device searches this table for a corresponding entry. When the device does not find a corresponding entry, it forwards the request.

**Table**

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

**Buttons**

- **Add**
  Adds a table row.

- **Remove**
  Removes the selected table row.

**Index**

Displays the index number to which the table row relates. The device automatically assigns the value when you add a table row.

**Name**

Specifies the hostname.

Possible values:
- Alphanumeric ASCII character string with 0..255 characters

**IP address**

Specifies the IP address under which the host is reachable.

Possible values:
- Valid IPv4 address (default setting: 0.0.0.0)

**Active**

Activates/deactivates the table row.

Possible values:
- **marked**
  The device resolves a request for the host name for this table row.
- **unmarked** (default setting)
  After receiving a request for this host name, the device sends a request to one of the configured name servers for resolution.
7.4 Industrial Protocols

The menu contains the following dialogs:

- IEC61850-MMS
- Modbus TCP
- OPC UA Server
### 7.4.1 IEC61850-MMS

The IEC61850-MMS is a standardized industrial communication protocol from the International Electrotechnical Commission (IEC). For example, automatic switching equipment uses this protocol when communicating with power station equipment.

The packet orientated protocol defines a uniform communication language based on the transport protocol, TCP/IP. The protocol uses a Manufacturing Message Specification (MMS) server for client server communications. The protocol includes functions for SCADA, Intelligent Electronic Device (IED) and the network control systems.

**Note:** IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and possible problems in the network.

Activate the write access only if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

This dialog lets you specify the following MMS server settings:
- Activates/deactivates the MMS server.
- Activates/deactivates the write access to the MMS server.
- The MMS server TCP Port.
- The maximum number of MMS server sessions.

### Operation

**Operation**

Enables/disables the IEC61850-MMS server.

Possible values:
- **On**
  - The IEC61850-MMS server is enabled.
- **Off** (default setting)
  - The IEC61850-MMS server is disabled.
  - The IEC61850 MIBs stay accessible.

### Information

**Status**

Displays the current IEC61850-MMS server status.

Possible values:
- **unavailable**
- **starting**
- **running**
- **stopping**
### Configuration

**Active sessions**
Displays the number of active MMS server connections.

**Buttons**

- **Download ICD file**
  Copies the ICD file to your PC.

**Write access**
Activates/deactivates the write access to the MMS server.

**Possible values:**
- **marked**
  The write access to the MMS server is activated. This setting lets you change the device settings using the IEC 61850 MMS protocol.
- **unmarked** (default setting)
  The write access to the MMS server is deactivated. The MMS server is accessible as read-only.

**Technical key**
Specifies the IED name.

- The IED name is eligible independently of the system name.

**Possible values:**
- Alphanumeric ASCII character string with 0..32 characters
  The device accepts the following characters:
  - –
  - 0..9
  - a..z
  - A..Z (default setting: KEY)

To get the MMS server to use the IED name, click the ✓ button and restart the MMS server. The connection to connected clients is then interrupted.

**TCP port**
Specifies TCP port for MMS server access.

**Possible values:**
- 1..65535 (default setting: 102)
  Exception: Port 2222 is reserved for internal functions.

**Note:** The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.
Sessions (max.)

Specifies the maximum number of MMS server connections.

Possible values:

- **1..15** (default setting: 5)
### 7.4.2 Modbus TCP

Modbus TCP is a protocol used for Supervisory Control and Data Acquisition (SCADA) system integration. Modbus TCP is a vendor-neutral protocol used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLC), sensors and meters.

This dialog lets you specify the parameters of the protocol. To monitor and control the parameters of the device, you need Human-Machine Interface (HMI) software and the memory mapping table. Refer to the tables located in the “Configuration” user manual for the supported objects and memory mapping.

The dialog lets you enable the function, activate the write access, control which TCP port the Human-Machine Interface (HMI) polls for data. You can also specify the number of sessions allowed to be open at the same time.

**Note:** Activating the Modbus TCP write-access can cause an unavoidable security risk, because the protocol does not authenticate user access.

To help minimize the unavoidable security risks, specify the IP address range located in the Device Security > Management Access dialog. Enter only the IP addresses assigned to your devices before enabling the function. Furthermore, the default setting for monitoring function activation in the Diagnostics > Status Configuration > Security Status dialog, Global tab, is active.

#### Operation

**Enables/disables the Modbus TCP server in the device.**

Possible values:
- **On**
  - The Modbus TCP server is enabled.
- **Off** (default setting)
  - The Modbus TCP server is disabled.

#### Configuration

**Write access**

Activates/deactivates the write access to the Modbus TCP parameters.

**Note:** Activating the Modbus TCP write-access can cause an unavoidable security risk, because the protocol does not authenticate user access.
Possible values:

- **marked** (default setting)
  - The *Modbus TCP* server read/write access is active. This lets you change the device configuration using the *Modbus TCP* protocol.

- **unmarked**
  - The *Modbus TCP* server read-only access is active.

### TCP port

Specifies the TCP port number that the *Modbus TCP* server uses for communication.

Possible values:

- `<TCP Port number>` (default setting: 502)
  - Specifying 0 is not allowed.

### Sessions (max.)

Specifies the maximum number of concurrent sessions that the *Modbus TCP* server maintains.

Possible values:

- 1..5 (default setting: 5)
7.4.3 **OPC UA Server**

The protocol **OPC UA** is a standardized protocol for industrial communication defined in the standard IEC 62541. The **OPC UA Server** function monitors the **OPC UA** information model data for the industrial automation equipments such as Programmable Logic Controllers (PLC), sensors and meters.

To monitor the **OPC UA** information model data of the connected end devices, use an **OPC UA** client application.

In this dialog you enable the **OPC UA Server** function and specify the required settings. You can also specify the number of sessions allowed to be open at the same time. The dialog lets you manage the **OPC UA** user accounts required to access the device using a **OPC UA** client application. Every **OPC UA** user requires an active **OPC UA** user account to gain access to the **OPC UA** server of the device.

**Operation**

**Operation** Enables/disables the **OPC UA Server** function in the device.

Possible values:

- **On**
  - The **OPC UA Server** function is enabled.

- **Off** (default setting)
  - The **OPC UA Server** function is disabled.

**Configuration**

**Configuration**

Specifies the TCP port number that the **OPC UA Server** server uses for communication.

Possible values:

- **1..65535** (default setting: **4840**)
  - Exception: Port **2222** is reserved for internal functions.
Sessions (max.)

Specifies the maximum number of OPC UA connections to the device that can be set up simultaneously. Each accessing OPC UA client application establishes a separate OPC UA connection to the device.

Possible values:

- **1..5** (default setting: 5)

Security policy

Specifies the authentication and encryption protocol that the device applies for the OPC UA user.

Possible values:

- **none** (default setting)
  - The OPC UA user does not need to authenticate oneself.
- **basic128Rsa15**
  - The OPC UA user authenticates using the Basic128Rsa15 protocol.
- **basic256**
  - The OPC UA user authenticates using the Basic256 protocol.
- **basic256Sha256**
  - The OPC UA user authenticates using the Basic256Sha256 protocol.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 16.

Buttons

**Add**

Opens the Create window to add a table row. The device lets you specify up to 4 OPC UA user accounts.

- In the **User name** field, you specify the name of the OPC UA user account.
  - Possible values:
    - Alphanumeric ASCII character string with 1..32 characters
    - The device accepts the following characters:
      - a..z
      - A..Z
      - 0..9
      - <space>
      - _

**Remove**

Removes the selected table row.

User name

Displays the name of the OPC UA user having access to the device using an OPC UA client application.
Password

Specifies the password that the user applies to access the device using an OPC UA client application.

Displays ***** (asterisks) instead of the password with which the user logs in. To change the password, click the relevant field.

Possible values:
- Alphanumeric ASCII character string with 6..64 characters
  The device accepts the following characters:
  - a..z
  - A..Z
  - 0..9
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

Access role

Specifies the role that regulates the access of the OPC UA user using an OPC UA client application.

Possible values:
- readOnly (default setting)
  The OPC UA user account has read-only access to the device. The OPC UA user can view the OPC UA information model data of the connected end devices.

Active

Activates/deactivates the OPC UA user account in the device.

Possible values:
- marked
  The OPC UA user account is active. The device accepts the login of an OPC UA user with this user name.
- unmarked (default setting)
  The OPC UA user account is inactive. The device rejects the login of an OPC UA user with this user name.
7.5 Command Line Interface

This dialog lets you access the device using the Command Line Interface.

Prerequisites:
- In the Device Security > Management Access > Server dialog, SSH tab the SSH server is enabled.
- On your workstation, install a SSH-capable client application which registers a handler for URLs starting with ssh:// in your operating system.

Buttons

Open SSH connection

Opens the SSH-capable client application.

When you click the button, the web application passes the URL of the device starting with ssh:// and the user name of the currently logged in user.

If the web browser finds a SSH-capable client application, then the SSH-capable client establishes a connection to the device using the SSH protocol.
## A Index

### 0-9
- 802.1D/p mapping ................................................. 209
- 802.1X .............................................................. 89, 129

### A
- Access control ...................................................... 129
- Access control lists ............................................. 158
- Access restriction ............................................... 115
- ACL ................................................................. 158
- Address conflict detection ..................................... 284
- Aging time .......................................................... 169, 288
- Alarms ................................................................. 277
- ARP ....................................................................... 284
- ARP table ............................................................. 288
- Audit trail .............................................................. 347
- Authentication history .......................................... 141
- Authentication list ................................................ 89
- Auto disable ......................................................... 125, 126, 231, 312, 313, 319, 334

### B
- Bridge ................................................................... 228

### C
- Cable diagnosis ..................................................... 307
- Certificate ............................................................. 21, 49, 95, 112, 113, 268, 294, 302
- CLI ......................................................................... 119
- Command line interface ........................................ 119
- Community names ................................................ 121
- Configuration check .............................................. 282
- Configuration profile ............................................ 16, 41
- Counter reset ......................................................... 68

### D
- Daylight saving time ............................................... 72
- Device software ..................................................... 38
- Device software backup ......................................... 38
- Device status ......................................................... 19, 258
- DHCP L2 relay ....................................................... 349
- DHCP server ......................................................... 354
- DHCPv6 L2 Relay .................................................... 349
- DNS ..................................................................... 363
- DNS cache ........................................................... 364
- DNS client ............................................................ 364
- Domain name system .............................................. 363
- DoS ..................................................................... 154
- DSCP .................................................................. 211
- Duplicate Address Detection ................................... 33

### E
- EAPOL ................................................................. 139
- Egress rate limiter .................................................. 172
- Email notification .................................................. 292
- Encryption ............................................................ 41
- ENVM .................................................................. 39, 41, 50, 53, 260, 266, 273, 344
- Event severity ....................................................... 296, 342
- External memory ................................................... 22, 39, 41, 50, 53, 344
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F</strong></td>
</tr>
<tr>
<td>FAQ</td>
</tr>
<tr>
<td>FDB</td>
</tr>
<tr>
<td>Filter MAC addresses</td>
</tr>
<tr>
<td>Fingerprint</td>
</tr>
<tr>
<td>Flash memory</td>
</tr>
<tr>
<td>Flow control</td>
</tr>
<tr>
<td>Forwarding database</td>
</tr>
<tr>
<td><strong>G</strong></td>
</tr>
<tr>
<td>GARP</td>
</tr>
<tr>
<td>GMRP</td>
</tr>
<tr>
<td>Guards</td>
</tr>
<tr>
<td>GVRP</td>
</tr>
<tr>
<td><strong>H</strong></td>
</tr>
<tr>
<td>Hardware clock</td>
</tr>
<tr>
<td>Hardware state</td>
</tr>
<tr>
<td>HiDiscovery</td>
</tr>
<tr>
<td>Host key</td>
</tr>
<tr>
<td>HTML</td>
</tr>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td>HTTP server</td>
</tr>
<tr>
<td>HTTPS</td>
</tr>
<tr>
<td><strong>I</strong></td>
</tr>
<tr>
<td>IAS</td>
</tr>
<tr>
<td>IEC61850-MMS</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
</tr>
<tr>
<td>IGMP snooping</td>
</tr>
<tr>
<td>Industrial HiVision</td>
</tr>
<tr>
<td>Ingress filtering</td>
</tr>
<tr>
<td>Ingress rate limiter</td>
</tr>
<tr>
<td>Integrated authentication server</td>
</tr>
<tr>
<td>IP access restriction</td>
</tr>
<tr>
<td>IP address conflict detection</td>
</tr>
<tr>
<td>IP DSCP mapping</td>
</tr>
<tr>
<td>IPv4 rule</td>
</tr>
<tr>
<td><strong>L</strong></td>
</tr>
<tr>
<td>L2 relay</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>Link aggregation</td>
</tr>
<tr>
<td>Link backup</td>
</tr>
<tr>
<td>LLDP</td>
</tr>
<tr>
<td>Load/save</td>
</tr>
<tr>
<td>Log file</td>
</tr>
<tr>
<td>Login banner</td>
</tr>
<tr>
<td>Loop protection</td>
</tr>
<tr>
<td>Loops</td>
</tr>
<tr>
<td>M</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>O</td>
</tr>
<tr>
<td>P</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Index

| S | Secure shell | 106 |
|   | Security status | 20, 263 |
|   | Self-test | 290 |
|   | Serial interface | 266 |
|   | Settings | 41 |
|   | Severity | 20, 269 |
|   | SFP module | 306 |
|   | Signal contact | 59, 64, 126, 228, 244, 258, 263, 269, 271, 277, 286, 288, 312 |
|   | SNMP traps | 121 |
|   | SNMP server | 104, 266 |
|   | SNMPv1/v2 | 75 |
|   | SNTP client | 76 |
|   | SNTP server | 80 |
|   | Software backup | 38 |
|   | Software update | 38 |
|   | Spanning tree protocol | 227 |
|   | SSH server | 106 |
|   | Subring | 251 |
|   | Support information (ZIP archive) | 342 |
|   | Syslog | 301 |
|   | System information | 250 |
|   | System log | 346 |
|   | System monitor | 290 |
|   | System time | 71 |
| T | Technical questions | 383 |
|   | Telnet server | 105, 265 |
|   | Temperature | 21, 259, 272 |
|   | Threshold values network load | 172 |
|   | Topology discovery | 330 |
|   | Training courses | 383 |
|   | Trap destination | 277 |
|   | Traps | 59, 64, 126, 228, 244, 258, 263, 271, 277, 286, 312 |
|   | Trust mode | 207 |
|   | Twisted pair | 307 |
| U | Unaware mode | 169 |
|   | USB network interface | 36 |
|   | User administration | 83 |
|   | Utilization | 60 |
| V | Virtual local area network | 214 |
|   | VLAN | 27, 214, 336 |
|   | VLAN configuration | 216 |
|   | VLAN ports | 219 |
|   | VLAN-unaware mode | 169 |
| W | Watchdog | 41, 43 |
|   | Web server | 110, 111 |
| Z | ZIP archive with support information | 342 |
B  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 [www.hirschmann.com](http://www.hirschmann.com).

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at [hirschmann-support.belden.com](http://hirschmann-support.belden.com). This site also includes a free of charge knowledge base and a software download section.

**Technical Documents**

The current manuals and operating instructions for Hirschmann products are available at [doc.hirschmann.com](http://doc.hirschmann.com).

**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.
- Support ranges from the first installation through the standby service to maintenance concepts.


With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.
C Readers’ Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a
description of our product as possible, as well as important information to assist you in the operation
of this product. Your comments and suggestions help us to further improve the quality of our
documentation.

Your assessment of this manual:

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Readability</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Understandability</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Examples</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Structure</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Comprehensive</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Graphics</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drawings</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tables</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Did you discover any errors in this manual?
If so, on what page?

________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

Suggestions for improvement and additional information:
General comments:

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page
► as a fax to the number +49 (0)7127/14-1600 or
► per mail to
  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany
User Manual

Configuration
GREYHOUND Switch GRS103
HiOS-2A
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.

© 2022 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

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 find the latest user documentation for your device at: doc.hirschmann.com

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety instructions</td>
<td>11</td>
</tr>
<tr>
<td>About this Manual</td>
<td>13</td>
</tr>
<tr>
<td>Key</td>
<td>14</td>
</tr>
<tr>
<td>Replacing a device</td>
<td>15</td>
</tr>
<tr>
<td><strong>1</strong> User interfaces</td>
<td></td>
</tr>
<tr>
<td>1.1 Graphical User Interface</td>
<td>17</td>
</tr>
<tr>
<td>1.2 Command Line Interface</td>
<td>17</td>
</tr>
<tr>
<td>1.2.1 Preparing the data connection</td>
<td>18</td>
</tr>
<tr>
<td>1.2.2 Access to the Command Line Interface using SSH (Secure Shell)</td>
<td>18</td>
</tr>
<tr>
<td>1.2.3 Access to the Command Line Interface using the serial interface</td>
<td>18</td>
</tr>
<tr>
<td>1.2.4 Mode-based command hierarchy</td>
<td>21</td>
</tr>
<tr>
<td>1.2.5 Executing the commands</td>
<td>22</td>
</tr>
<tr>
<td>1.2.6 Structure of a command</td>
<td>26</td>
</tr>
<tr>
<td>1.2.7 Examples of commands</td>
<td>26</td>
</tr>
<tr>
<td>1.2.8 Input prompt</td>
<td>29</td>
</tr>
<tr>
<td>1.2.9 Key combinations</td>
<td>30</td>
</tr>
<tr>
<td>1.2.10 Data entry elements</td>
<td>31</td>
</tr>
<tr>
<td>1.2.11 Use cases</td>
<td>33</td>
</tr>
<tr>
<td>1.2.12 Service Shell</td>
<td>34</td>
</tr>
<tr>
<td>1.3 System monitor</td>
<td>35</td>
</tr>
<tr>
<td>1.3.1 Functional scope</td>
<td>38</td>
</tr>
<tr>
<td>1.3.2 Starting the System Monitor</td>
<td>38</td>
</tr>
<tr>
<td><strong>2</strong> Specifying the IP parameters</td>
<td></td>
</tr>
<tr>
<td>2.1 IP parameter basics</td>
<td>41</td>
</tr>
<tr>
<td>2.1.1 IPv4</td>
<td>41</td>
</tr>
<tr>
<td>2.1.2 IPv6</td>
<td>45</td>
</tr>
<tr>
<td>2.2 Specifying the IP parameters using the Command Line Interface</td>
<td>50</td>
</tr>
<tr>
<td>2.2.1 IPv4</td>
<td>50</td>
</tr>
<tr>
<td>2.2.2 IPv6</td>
<td>51</td>
</tr>
<tr>
<td>2.3 Specifying the IP parameters using HiDiscovery</td>
<td>53</td>
</tr>
<tr>
<td>2.4 Specifying the IP parameters using the Graphical User Interface</td>
<td>55</td>
</tr>
<tr>
<td>2.4.1 IPv4</td>
<td>55</td>
</tr>
<tr>
<td>2.4.2 IPv6</td>
<td>56</td>
</tr>
<tr>
<td>2.5 Specifying the IP parameters using BOOTP</td>
<td>57</td>
</tr>
<tr>
<td>2.6 Specifying the IP parameters using DHCP</td>
<td>58</td>
</tr>
<tr>
<td>2.6.1 IPv4</td>
<td>58</td>
</tr>
<tr>
<td>2.6.2 IPv6</td>
<td>59</td>
</tr>
<tr>
<td>2.7 Management address conflict detection</td>
<td>61</td>
</tr>
<tr>
<td>2.7.1 Active and passive detection</td>
<td>61</td>
</tr>
<tr>
<td>2.8 Duplicate Address Detection</td>
<td>62</td>
</tr>
<tr>
<td><strong>3</strong> Access to the device</td>
<td></td>
</tr>
<tr>
<td>3.1 Access roles</td>
<td>63</td>
</tr>
<tr>
<td>3.2 First login (Password change)</td>
<td>64</td>
</tr>
</tbody>
</table>

**About this Manual**

Software: UM Config GRS

Release: 9.1 08/2022
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3 Authentication lists</td>
<td>65</td>
</tr>
<tr>
<td>3.3.1 Applications</td>
<td>65</td>
</tr>
<tr>
<td>3.3.2 Policies</td>
<td>65</td>
</tr>
<tr>
<td>3.3.3 Managing authentication lists</td>
<td>65</td>
</tr>
<tr>
<td>3.3.4 Adjust the settings</td>
<td>66</td>
</tr>
<tr>
<td>3.4 User management</td>
<td>68</td>
</tr>
<tr>
<td>3.4.1 Access roles</td>
<td>68</td>
</tr>
<tr>
<td>3.4.2 Managing user accounts</td>
<td>70</td>
</tr>
<tr>
<td>3.4.3 Default setting</td>
<td>70</td>
</tr>
<tr>
<td>3.4.4 Changing default passwords</td>
<td>70</td>
</tr>
<tr>
<td>3.4.5 Setting up a new user account</td>
<td>71</td>
</tr>
<tr>
<td>3.4.6 Deactivating the user account</td>
<td>72</td>
</tr>
<tr>
<td>3.4.7 Adjusting policies for passwords</td>
<td>73</td>
</tr>
<tr>
<td>3.5 LDAP</td>
<td>75</td>
</tr>
<tr>
<td>3.5.1 Coordination with the server administrator</td>
<td>75</td>
</tr>
<tr>
<td>3.5.2 Example configuration</td>
<td>76</td>
</tr>
<tr>
<td>3.6 SNMP access</td>
<td>79</td>
</tr>
<tr>
<td>3.6.1 SNMPv1/v2 access</td>
<td>79</td>
</tr>
<tr>
<td>3.6.2 SNMPv3 access</td>
<td>79</td>
</tr>
<tr>
<td>3.7 Out-of-Band access</td>
<td>81</td>
</tr>
<tr>
<td>3.7.1 Specifying the IP parameters</td>
<td>81</td>
</tr>
<tr>
<td>3.7.2 Disable the USB network interface</td>
<td>82</td>
</tr>
<tr>
<td>4 Synchronizing the system time in the network</td>
<td>83</td>
</tr>
<tr>
<td>4.1 Basic settings</td>
<td>83</td>
</tr>
<tr>
<td>4.1.1 Setting the time</td>
<td>83</td>
</tr>
<tr>
<td>4.1.2 Automatic daylight saving time changeover</td>
<td>85</td>
</tr>
<tr>
<td>4.2 SNTP</td>
<td>86</td>
</tr>
<tr>
<td>4.2.1 Preparation</td>
<td>87</td>
</tr>
<tr>
<td>4.2.2 Defining settings of the SNTP client</td>
<td>88</td>
</tr>
<tr>
<td>4.2.3 Specifying SNTP server settings</td>
<td>89</td>
</tr>
<tr>
<td>5 Managing configuration profiles</td>
<td>91</td>
</tr>
<tr>
<td>5.1 Detecting changed settings</td>
<td>91</td>
</tr>
<tr>
<td>5.1.1 Volatile memory (RAM) and non-volatile memory (NVM)</td>
<td>91</td>
</tr>
<tr>
<td>5.1.2 External memory (ACA) and non-volatile memory (NVM)</td>
<td>92</td>
</tr>
<tr>
<td>5.2 Saving the settings</td>
<td>93</td>
</tr>
<tr>
<td>5.2.1 Saving the configuration profile in the device</td>
<td>93</td>
</tr>
<tr>
<td>5.2.2 Saving the configuration profile in the external memory</td>
<td>95</td>
</tr>
<tr>
<td>5.2.3 Backup the configuration profile on a remote server</td>
<td>95</td>
</tr>
<tr>
<td>5.2.4 Exporting a configuration profile</td>
<td>96</td>
</tr>
<tr>
<td>5.3 Loading settings</td>
<td>98</td>
</tr>
<tr>
<td>5.3.1 Activating a configuration profile</td>
<td>98</td>
</tr>
<tr>
<td>5.3.2 Loading the configuration profile from the external memory</td>
<td>98</td>
</tr>
<tr>
<td>5.3.3 Importing a configuration profile</td>
<td>100</td>
</tr>
<tr>
<td>5.4 Reset the device to the factory defaults</td>
<td>103</td>
</tr>
<tr>
<td>5.4.1 Using the Graphical User Interface or Command Line Interface</td>
<td>103</td>
</tr>
<tr>
<td>5.4.2 Using the System Monitor</td>
<td>103</td>
</tr>
<tr>
<td>6 Loading software updates</td>
<td>105</td>
</tr>
<tr>
<td>6.1 Loading a previous software version</td>
<td>105</td>
</tr>
<tr>
<td>6.2 Software update from the PC</td>
<td>106</td>
</tr>
<tr>
<td>6.3 Software update from a server</td>
<td>107</td>
</tr>
</tbody>
</table>
6.4 Software update from the external memory ................................................. 108
6.4.1 Manually—initiated by the administrator ............................................. 108
6.4.2 Automatically—initiated by the device ................................................... 108

7 Configuring the ports .................................................................................. 111
7.1 Enabling/disabling the port ....................................................................... 111
7.2 Selecting the operating mode ..................................................................... 112

8 Assistance in the protection from unauthorized access .................................. 113
8.1 Changing the SNMPv1/v2 community ....................................................... 113
8.2 Disabling SNMPv1/v2 ............................................................................ 114
8.3 Disabling HTTP ....................................................................................... 115
8.4 Disabling Telnet ....................................................................................... 116
8.5 Disabling the HiDiscovery access ............................................................. 117
8.6 Activating the IP access restriction ........................................................... 118
8.7 Adjusting the session timeouts ................................................................. 120
8.8 Deactivating the unused modules ............................................................. 122

9 Controlling the data traffic ......................................................................... 123
9.1 Helping protect against DoS attacks ........................................................... 123
9.1.1 Filters for TCP and UDP packets ......................................................... 124
9.1.2 Filters for IP packets ........................................................................... 128
9.1.3 Filters for ICMP packets .................................................................... 128
9.2 ACL ........................................................................................................... 130
9.2.1 Creating and editing IPv4 rules .............................................................. 131
9.2.2 Creating and configuring an IP ACL using the Command Line Interface ........................................... 132
9.2.3 Creating and editing MAC rules ........................................................... 132
9.2.4 Creating and configuring a MAC ACL using the Command Line Interface ........................................ 133
9.2.5 Assigning ACLs to a port or VLAN ..................................................... 134

10 Network load control .............................................................................. 135
10.1 Direct packet distribution ....................................................................... 135
10.1.1 Learning MAC addresses ................................................................... 135
10.1.2 Aging of learned MAC addresses ....................................................... 135
10.1.3 Static address entries ........................................................................ 135
10.2 Multicasts .................................................................................................. 139
10.2.1 Example of a Multicast application ..................................................... 139
10.2.2 IGMP snooping ................................................................................... 139
10.3 Rate limiter ................................................................................................ 144
10.4 QoS/Priority ............................................................................................. 145
10.4.1 Description of prioritization ................................................................. 145
10.4.2 Handling of received priority information .......................................... 146
10.4.3 VLAN tagging .................................................................................... 146
10.4.4 IP ToS (Type of Service) ................................................................... 147
10.4.5 Handling of traffic classes ................................................................. 148
10.4.6 Queue management ........................................................................... 149
10.4.7 Management prioritization ................................................................. 150
10.4.8 Setting prioritization .......................................................................... 150
10.5 Flow control ............................................................................................. 154
10.5.1 Halfduplex or fullduplex link .............................................................. 154
10.5.2 Setting up the Flow Control ............................................................... 155

Contents
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>VLANs</td>
<td>157</td>
</tr>
<tr>
<td>11.1</td>
<td>Examples of VLANs</td>
<td>157</td>
</tr>
<tr>
<td>11.1.1</td>
<td>Example 1</td>
<td>158</td>
</tr>
<tr>
<td>11.1.2</td>
<td>Example 2</td>
<td>161</td>
</tr>
<tr>
<td>11.2</td>
<td>Guest VLAN / Unauthenticated VLAN</td>
<td>166</td>
</tr>
<tr>
<td>11.3</td>
<td>RADIUS VLAN assignment</td>
<td>168</td>
</tr>
<tr>
<td>11.4</td>
<td>Creating a Voice VLAN</td>
<td>169</td>
</tr>
<tr>
<td>11.5</td>
<td>VLAN unaware mode</td>
<td>170</td>
</tr>
<tr>
<td>12</td>
<td>Redundancy</td>
<td>171</td>
</tr>
<tr>
<td>12.1</td>
<td>Network Topology vs. Redundancy Protocols</td>
<td>171</td>
</tr>
<tr>
<td>12.1.1</td>
<td>Network topologies</td>
<td>171</td>
</tr>
<tr>
<td>12.1.2</td>
<td>Redundancy Protocols</td>
<td>172</td>
</tr>
<tr>
<td>12.1.3</td>
<td>Combinations of redundancy protocols</td>
<td>173</td>
</tr>
<tr>
<td>12.2</td>
<td>Media Redundancy Protocol (MRP)</td>
<td>174</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Network Structure</td>
<td>174</td>
</tr>
<tr>
<td>12.2.2</td>
<td>Reconfiguration time</td>
<td>175</td>
</tr>
<tr>
<td>12.2.3</td>
<td>Advanced mode</td>
<td>175</td>
</tr>
<tr>
<td>12.2.4</td>
<td>Prerequisites for MRP</td>
<td>175</td>
</tr>
<tr>
<td>12.2.5</td>
<td>Advanced Information</td>
<td>176</td>
</tr>
<tr>
<td>12.2.6</td>
<td>Example Configuration</td>
<td>177</td>
</tr>
<tr>
<td>12.2.7</td>
<td>MRP over LAG</td>
<td>181</td>
</tr>
<tr>
<td>12.3</td>
<td>Spanning Tree</td>
<td>185</td>
</tr>
<tr>
<td>12.3.1</td>
<td>Basics</td>
<td>185</td>
</tr>
<tr>
<td>12.3.2</td>
<td>Rules for Creating the Tree Structure</td>
<td>189</td>
</tr>
<tr>
<td>12.3.3</td>
<td>Examples</td>
<td>191</td>
</tr>
<tr>
<td>12.4</td>
<td>Rapid Spanning Tree Protocol</td>
<td>194</td>
</tr>
<tr>
<td>12.4.1</td>
<td>Port roles</td>
<td>194</td>
</tr>
<tr>
<td>12.4.2</td>
<td>Port states</td>
<td>195</td>
</tr>
<tr>
<td>12.4.3</td>
<td>Spanning Tree Priority Vector</td>
<td>196</td>
</tr>
<tr>
<td>12.4.4</td>
<td>Fast reconfiguration</td>
<td>196</td>
</tr>
<tr>
<td>12.4.5</td>
<td>Configuring the device</td>
<td>197</td>
</tr>
<tr>
<td>12.4.6</td>
<td>Guards</td>
<td>199</td>
</tr>
<tr>
<td>12.5</td>
<td>Link Aggregation</td>
<td>203</td>
</tr>
<tr>
<td>12.5.1</td>
<td>Methods of Operation</td>
<td>203</td>
</tr>
<tr>
<td>12.5.2</td>
<td>Link Aggregation Example</td>
<td>203</td>
</tr>
<tr>
<td>12.6</td>
<td>Link Backup</td>
<td>205</td>
</tr>
<tr>
<td>12.6.1</td>
<td>Fail Back Description</td>
<td>205</td>
</tr>
<tr>
<td>12.6.2</td>
<td>Example Configuration</td>
<td>205</td>
</tr>
<tr>
<td>12.7</td>
<td>FuseNet</td>
<td>207</td>
</tr>
<tr>
<td>12.8</td>
<td>Sub Ring</td>
<td>208</td>
</tr>
<tr>
<td>12.8.1</td>
<td>Sub Ring description</td>
<td>208</td>
</tr>
<tr>
<td>12.8.2</td>
<td>Advanced Information</td>
<td>210</td>
</tr>
<tr>
<td>12.8.3</td>
<td>Sub Ring example</td>
<td>211</td>
</tr>
<tr>
<td>12.8.4</td>
<td>Sub Ring example configuration</td>
<td>213</td>
</tr>
<tr>
<td>12.9</td>
<td>Sub Ring with LAG</td>
<td>215</td>
</tr>
<tr>
<td>12.9.1</td>
<td>Example</td>
<td>215</td>
</tr>
</tbody>
</table>
13 Operation diagnosis ......................................................... 219
  13.1 Sending SNMP traps ...................................................... 219
  13.1.1 List of SNMP traps ..................................................... 219
  13.1.2 SNMP traps for configuration activity ......................... 220
  13.1.3 SNMP trap setting ..................................................... 221
  13.1.4 ICMP messaging ....................................................... 222
  13.2 Monitoring the Device Status ......................................... 223
  13.2.1 Events which can be monitored ................................. 223
  13.2.2 Configuring the Device Status .................................... 224
  13.2.3 Displaying the Device Status .................................... 225
  13.3 Security Status .......................................................... 227
  13.3.1 Events which can be monitored ................................. 227
  13.3.2 Configuring the Security Status ................................. 228
  13.3.3 Displaying the Security Status .................................. 229
  13.4 Out-of-Band signaling .................................................. 230
  13.5 Port event counter ....................................................... 231
  13.6 Auto-Disable ............................................................. 231
  13.7 Displaying the SFP status .............................................. 231
  13.8 Topology discovery ...................................................... 232
  13.9 Detecting loops .......................................................... 232
  13.10 Help protect against layer 2 network loops ..................... 233
  13.10.1 Application example ................................................. 233
  13.10.2 Recommendations for redundant ports ....................... 234
  13.11 Using the Email Notification function .......................... 235
  13.11.1 Specify the sender address ......................................... 235
  13.11.2 Specify the triggering events ................................. 236
  13.11.3 Change the send interval ....................................... 236
  13.11.4 Specify the recipients ........................................... 237
  13.11.5 Specify the mail server .......................................... 238
  13.11.6 Enable/disable the Email Notification function ............. 238
  13.11.7 Send a test email .................................................. 239
  13.12 Reports ................................................................. 239
  13.12.1 Global settings ..................................................... 240
  13.12.2 Syslog ............................................................... 240
  13.12.3 System Log .......................................................... 241
  13.12.4 Syslog over TLS .................................................... 241
  13.12.5 Audit Trail .......................................................... 242
  13.13 Network analysis with TCPdump .................................... 243
  13.14 Monitoring the data traffic .......................................... 243
  13.14.1 Port Mirroring ....................................................... 244
  13.15 Self-test ............................................................... 244
  13.16 Copper cable test ...................................................... 245

UM Config GRS
Release 9.1 08/2022
14  Advanced functions of the device

14.1 Using the device as a DHCP server.

14.1.1 IP Addresses assigned per port or per VLAN

14.1.2 DHCP server static IP address example

14.1.3 DHCP server dynamic IP address range example.

14.2 DHCP L2 Relay

14.2.1 Circuit and Remote IDs

14.2.2 DHCP L2 Relay configuration

14.3 Using the device as a DNS client.

14.3.1 Configuring a DNS server example

14.4 GARP

14.4.1 Configuring GMRP

14.4.2 Configuring GVRP

14.5 MRP-IEEE

14.5.1 MRP operation

14.5.2 MRP timers

14.5.3 MMRP

14.5.4 MVRP

15  Industry Protocols

15.1 IEC 61850/MMS

15.1.1 Switch model for IEC 61850.

15.1.2 Integration into a Control System.

15.2 Modbus TCP

15.2.1 Client/Server Modbus TCP/IP Mode

15.2.2 Supported Functions and Memory Mapping

15.2.3 Example Configuration

15.3 OPC UA Server

15.3.1 Enabling the OPC UA server

15.3.2 Setting up an OPC UA user account

15.3.3 Deactivating an OPC UA user account

15.3.4 Delete an OPC UA user account

A  Setting up the configuration environment

A.1 Setting up a DHCP/BOOTP server

A.2 Setting up a DHCP server with Option 82

A.3 Preparing access using SSH

A.3.1 Generating a key in the device

A.3.2 Loading your own key onto the device

A.3.3 Preparing the SSH client program

A.4 HTTPS certificate

A.4.1 HTTPS certificate management

A.4.2 Access through HTTPS

B  Appendix

B.1 Literature references

B.2 Maintenance

B.3 Management Information Base (MIB)

B.4 List of RFCs

B.5 Underlying IEEE Standards

B.6 Underlying IEC Norms

B.7 Underlying ANSI Norms
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.8</td>
<td>Technical Data</td>
<td>320</td>
</tr>
<tr>
<td>15.3.5</td>
<td>Switching</td>
<td>320</td>
</tr>
<tr>
<td>15.3.6</td>
<td>VLAN</td>
<td>320</td>
</tr>
<tr>
<td>15.3.7</td>
<td>Access Control Lists (ACL)</td>
<td>320</td>
</tr>
<tr>
<td>B.9</td>
<td>Copyright of integrated Software</td>
<td>321</td>
</tr>
<tr>
<td>B.10</td>
<td>Abbreviations used.</td>
<td>322</td>
</tr>
<tr>
<td>C</td>
<td>Index</td>
<td>325</td>
</tr>
<tr>
<td>D</td>
<td>Further support</td>
<td>331</td>
</tr>
<tr>
<td>E</td>
<td>Readers’ Comments</td>
<td>332</td>
</tr>
</tbody>
</table>
### Safety instructions

<table>
<thead>
<tr>
<th>![WARNING]</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNCONTROLLED MACHINE ACTIONS</strong></td>
<td></td>
</tr>
<tr>
<td>To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.</td>
<td></td>
</tr>
<tr>
<td>Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.</td>
<td></td>
</tr>
<tr>
<td><strong>Failure to follow these instructions can result in death, serious injury, or equipment damage.</strong></td>
<td></td>
</tr>
</tbody>
</table>
About this Manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway
**Key**

The designations used in this manual have the following meanings:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️</td>
<td>List</td>
</tr>
<tr>
<td>□</td>
<td>Work step</td>
</tr>
<tr>
<td>Link</td>
<td>Cross-reference with link</td>
</tr>
</tbody>
</table>

**Note:** A note emphasizes a significant fact or draws your attention to a dependency.

**Courier:** Representation of a CLI command or field contents in the graphical user interface

- Execution in the Graphical User Interface
- Execution in the Command Line Interface
Replacing a device

The device provides the following plug-and-play solutions for replacing a device with a device of the same type, for instance, if a failure was detected or for preventive maintenance:

- The new device loads the configuration profile of the replaced device from the external memory. See “Loading the configuration profile from the external memory” on page 98.
- The new device gets its IP address using DHCP Option 82. See “DHCP L2 Relay” on page 266. See “Setting up a DHCP server with Option 82” on page 302.

With each solution, upon reboot, the new device gets the same IP settings that the replaced device had.

- For accessing the device management using HTTPS, the device uses a digital certificate. You have the option to import your own certificate to the device. See “HTTPS certificate management” on page 308.
- For accessing the device management using SSH, the device uses an RSA host key. You have the option to import your own host key in PEM format to the device. See “Loading your own key onto the device” on page 305.
1 User interfaces

The device lets you specify the settings of the device using the following user interfaces.

<table>
<thead>
<tr>
<th>User interface</th>
<th>Can be reached through …</th>
<th>Prerequisite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphical User Interface</td>
<td>Ethernet (In-Band)</td>
<td>Web browser</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>Ethernet (In-Band)</td>
<td>Terminal emulation software</td>
</tr>
<tr>
<td></td>
<td>Serial interface (Out-of-Band)</td>
<td></td>
</tr>
<tr>
<td>System monitor</td>
<td>Serial interface (Out-of-Band)</td>
<td>Terminal emulation software</td>
</tr>
</tbody>
</table>

1.1 Graphical User Interface

System requirements

To open the Graphical User Interface, you need the desktop version of a web browser with HTML5 support.

Note: Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic recommendations. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

Starting the Graphical User Interface

The prerequisite for starting the Graphical User Interface is that the IP parameters are configured in the device. See “Specifying the IP parameters” on page 41.

Perform the following steps:

☐ Start your web browser.
☐ Type the IP address of the device in the address field of the web browser.
  Use the following form: https://xxx.xxx.xxx.xxx
  The web browser sets up the connection to the device and displays the login dialog.
☐ When you want to change the language of the Graphical User Interface, click the appropriate link in the top right corner of the login dialog.
☐ Enter the user name.
☐ Enter the password.
  The default password is private.
  After you enter the default password for the first time, the device will prompt you to assign a new password.
☐ Click the Login button.
  The web browser displays the Graphical User Interface.
1.2 Command Line Interface

The Command Line Interface lets you use the functions of the device through a local or remote connection.

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you have knowledge about the basics and about using Hirschmann devices.

1.2.1 Preparing the data connection

Information for assembling and starting up your device can be found in the “Installation” user manual.

☐ Connect the device with the network. The prerequisite for a successful data connection is the correct setting of the network parameters.

You can access the user interface of the Command Line Interface for example, with the freeware program PuTTY. You can download the software from www.putty.org.

☐ Install the PuTTY program on your computer.

1.2.2 Access to the Command Line Interface using SSH (Secure Shell)

In the following example we use the PuTTY program. Another option to access your device using SSH is the OpenSSH Suite.

Perform the following steps:

☐ Start the PuTTY program on your computer.

Figure 1: PuTTY input screen
In the Host Name (or IP address) field you enter the IP address of your device. The IP address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.

To specify the connection type, select the SSH radio button in the Connection type option list. After selecting and setting the required parameters, the device lets you set up the data connection using SSH.

Click the Open button to set up the data connection to your device. Depending on the device and the time at which SSH was configured, setting up the connection takes up to a minute.

When you first log in, towards the end of the connection setup, the PuTTY program displays a security alert message and lets you check the fingerprint of the key.

![PuTTY Security Alert](image)

Figure 2: Security alert prompt for the fingerprint

Check the fingerprint.

This helps protect yourself from unwelcome guests.

When the fingerprint matches the fingerprint of the device key, click the Yes button.

The device lets you display the finger prints of the device keys with the command `show ssh` or in the Device Security > Management Access > Server dialog, SSH tab.

The Command Line Interface appears on the screen with a window for entering the user name. The device enables up to 5 users to have access to the Command Line Interface at the same time.

Enter the user name.

The default user name is admin.

Press the <Enter> key.
Enter the password.
The default password is private.
After you enter the default password for the first time, the device will prompt you to assign a new password.

Press the <Enter> key.

login as: admin
admin@192.168.1.5's password:

Copyright (c) 2011-2022 Hirschmann Automation and Control GmbH
All rights reserved
GRS103 Release HiOS-2A-09.1.00
(Build date 2022-08-23 09:03)

System Name  :  GRS103-ECE555d5e786
Management IP :  192.168.1.5
Subnet Mask   :  255.255.255.0
Base MAC      :  EC:E5:55:01:02:03
USB IP        :  192.168.248.100
USB Mask      :  255.255.255.0
System Time   :  2022-08-25 12:15:23

NOTE: Enter '?' for Command Help. Command help displays all options that are valid for the particular mode.
For the syntax of a particular command form, please consult the documentation.

GRS>

Figure 3: Start screen of the Command Line Interface
1.2.3 Access to the Command Line Interface using the serial interface

The serial interface is used to locally connect an external network management station (VT100 terminal or PC with terminal emulation). The interface lets you set up a data connection to the Command Line Interface and to the system monitor.

Perform the following steps:

- Connect the device to a terminal using the serial interface. Alternatively connect the device to a COM port of your PC using terminal emulation based on VT100 and press any key.
- Alternatively you set up the serial data connection to the device with the serial interface using the PuTTY program. Press the <Enter> key.

- Press any key on your terminal keyboard a number of times until the login screen indicates the CLI mode.
- Enter the user name. The default user name is admin.
- Press the <Enter> key.
Enter the password. The default password is `private`. After you enter the default password for the first time, the device will prompt you to assign a new password.

Press the <Enter> key.

---

1.2.4 Mode-based command hierarchy

In the Command Line Interface, the commands are grouped in the related modes, according to the type of the command. Every command mode supports specific Hirschmann software commands.

The commands available to you as a user depend on your privilege level (`administrator`, `operator`, `guest`, `auditor`). They also depend on the mode in which you are currently working. When you switch to a specific mode, the commands of the mode are available to you.

The User Exec mode commands are an exception. The Command Line Interface also lets you execute these commands in the Privileged Exec mode.
The following figure displays the modes of the Command Line Interface.

![Diagram of Command Line Interface modes]

**User Exec mode**
When you log in with the Command Line Interface, you are in the User Exec mode. The User Exec mode contains a limited range of commands.
Command prompt: (GRS) >

**Privileged Exec mode**
To access the entire range of commands, you change to the Privileged Exec mode. The prerequisite for changing to the Privileged Exec mode is that you log in as a privileged user. In the Privileged Exec mode, you are able to execute the User Exec mode commands, too.
Command prompt: (GRS) #

**VLAN mode**
The VLAN mode contains VLAN-related commands.
Command prompt: (GRS) (VLAN) #

**Service Shell**
The Service Shell is for service purposes only.
Command prompt: /mnt/fastpath #
User interfaces
1.2 Command Line Interface

- Global Config mode
  The Global Config mode lets you perform modifications to the current configuration. This mode groups general setup commands.
  Command prompt: (GRS) (config)#

- Interface Range mode
  The commands in the Interface Range mode affect a specific port, a selected group of multiple ports or all port of the device. The commands modify a value or switch a function on/off on one or more specific ports.
  - All physical ports in the device
    Command prompt: (GRS) ((interface) all)#
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    (GRS) (config)#interface all
    (GRS) ((Interface)all)#
  - A single port on one interface
    Command prompt: (GRS) (interface <slot/port>)#
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    (GRS) (config)#interface 2/1
    (GRS) (interface 2/1)#
  - A range of ports on one interface
    Command prompt: (GRS) (interface <interface range>)#
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    (GRS) (config)#interface 1/2-1/4
    (GRS) ((Interface)1/2-1/4)#
  - A list of single ports
    Command prompt: (GRS) (interface <interface list>)#
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    (GRS) (config)#interface 1/2,1/4,1/5
    (GRS) ((Interface)1/2,1/4,1/5)#
  - A list of port ranges and single ports
    Command prompt: (GRS) (interface <complex range>)#
    Example: When you switch from the Global Config mode to the Interface Range mode, the command prompt changes as follows:
    (GRS) (config)#interface 1/2-1/4,1/6-1/9
    (GRS) ((Interface)1/2-1/4,1/6-1/9)

The following table displays the command modes, the command prompts (input request characters) visible in the corresponding mode, and the option with which you quit this mode.

Table 2: Command modes

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Access method</th>
<th>Quit or start next mode</th>
</tr>
</thead>
</table>
| User Exec mode        | First access level. Perform basic tasks and list system information. | To quit you enter `logout`:  
  (GRS) >logout  
  Are you sure (Y/N) ?y |
| Privileged Exec mode  | From the User Exec mode, you enter the command `enable`:  
  (GRS) >enable  
  (GRS) #           | To quit the Privileged Exec mode and return to the User Exec mode, you enter `exit`:  
  (GRS) #exit  
  (GRS) >          |
**Table 2: Command modes**

<table>
<thead>
<tr>
<th>Command mode</th>
<th>Access method</th>
<th>Quit or start next mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN mode</td>
<td>From the Privileged Exec mode, you enter the command <code>vlan database</code>:</td>
<td>To end the VLAN mode and return to the Privileged Exec mode, you enter <code>exit</code> or press Ctrl Z.</td>
</tr>
<tr>
<td></td>
<td>(GRS) #vlan database</td>
<td>(GRS) (Vlan)#</td>
</tr>
<tr>
<td></td>
<td>(GRS) (Vlan)#</td>
<td></td>
</tr>
<tr>
<td>Global Config mode</td>
<td>From the Privileged Exec mode, you enter the command <code>configure</code>:</td>
<td>To quit the Global Config mode and return to the Privileged Exec mode, you enter <code>exit</code>:</td>
</tr>
<tr>
<td></td>
<td>(GRS) #configure</td>
<td>(GRS) (config)#</td>
</tr>
<tr>
<td></td>
<td>(GRS) (config)#</td>
<td>To then quit the Privileged Exec mode and return to the User Exec mode, you enter <code>exit</code> again:</td>
</tr>
<tr>
<td></td>
<td>From the User Exec mode, you enter the command <code>enable</code>, and then in Privileged Exec mode, enter the command <code>configure</code>:</td>
<td>(GRS) &gt;enable</td>
</tr>
<tr>
<td></td>
<td>(GRS) &gt;enable</td>
<td>(GRS) #exit</td>
</tr>
<tr>
<td></td>
<td>(GRS) #configure</td>
<td>(GRS) &gt;</td>
</tr>
<tr>
<td></td>
<td>(GRS) (config)#</td>
<td></td>
</tr>
<tr>
<td>Interface Range mode</td>
<td>From the Global Config mode you enter the command <code>interface</code></td>
<td>To quit the Interface Range mode and return to the Global Config mode, you enter <code>exit</code>.</td>
</tr>
<tr>
<td></td>
<td>`{all</td>
<td>&lt;slot/port&gt;</td>
</tr>
<tr>
<td></td>
<td>(GRS) (config)#interface <code>&lt;slot/port&gt;</code></td>
<td>(GRS) (interface slot/port)#</td>
</tr>
<tr>
<td></td>
<td>(GRS) (interface slot/port)#</td>
<td>(GRS) #</td>
</tr>
</tbody>
</table>

When you enter a question mark (?) after the prompt, the Command Line Interface displays a list of the available commands and a short description of the commands.

**Figure 7: Commands in the User Exec mode**

```plaintext
(GRS)>
c11                Set the CLI preferences.
enable             Turn on privileged commands.
help               Display help for various special keys.
history            Show a list of previously run commands.
logout             Exit this session.
ping               Send ICMP echo packets to a specified IP address.
show               Display device options and settings.
telnet             Establish a telnet connection to a remote host.
```
1.2.5 Executing the commands

Syntax analysis

When you log in with the Command Line Interface, you are in the User Exec mode. The Command Line Interface displays the prompt (GRS)> on the screen.

When you enter a command and press the <Enter> key, the Command Line Interface starts the syntax analysis. The Command Line Interface searches the command tree for the desired command.

When the command is outside the Command Line Interface command range, a message informs you of the detected error.

Example:

You want to execute the show system info command, but enter info without f and press the <Enter> key.

The Command Line Interface then displays a message:

(GRS)>show system ino

Error: Invalid command 'ino'

Command tree

The commands in the Command Line Interface are organized in a tree structure. The commands, and where applicable the related parameters, branch down until the command is completely defined and therefore executable. The Command Line Interface checks the input. When you entered the command and the parameters correctly and completely, you execute the command with the <Enter> key.

After you entered the command and the required parameters, the other parameters entered are treated as optional parameters. When one of the parameters is unknown, the Command Line Interface displays a syntax message.

The command tree branches for the required parameters until the required parameters have reached the last branch in the structure.

With optional parameters, the command tree branches until the required parameters and the optional parameters have reached the last branch in the structure.

1.2.6 Structure of a command

This section describes the syntax, conventions and terminology, and uses examples to represent them.
Format of commands

Most of the commands include parameters.

When the command parameter is missing, the Command Line Interface informs you about the detection of an incorrect command syntax.

This manual displays the commands and parameters in the Courier font.

Parameters

The sequence of the parameters is relevant for the correct syntax of a command.

Parameters are required values, optional values, selections, or a combination of these things. The representation indicates the type of the parameter.

Table 3: Parameter and command syntax

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;command&gt;</td>
<td>Commands in pointed brackets (&lt;&gt; ) are obligatory.</td>
</tr>
<tr>
<td>[command]</td>
<td>Commands in square brackets ([ ]) are optional.</td>
</tr>
<tr>
<td>&lt;parameter&gt;</td>
<td>Parameters in pointed brackets (&lt;&gt; ) are obligatory.</td>
</tr>
<tr>
<td>[parameter]</td>
<td>Parameters in square brackets ([ ]) are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element.</td>
</tr>
<tr>
<td>[Choice1</td>
<td>Choice2]</td>
</tr>
<tr>
<td>{list}</td>
<td>Curved brackets ({ }) indicate that a parameter is to be selected from a list of options.</td>
</tr>
<tr>
<td>{Choice1</td>
<td>Choice2}</td>
</tr>
<tr>
<td>[param1 {Choice1</td>
<td>Choice2}]</td>
</tr>
<tr>
<td>&lt;a.b.c.d&gt;</td>
<td>Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)</td>
</tr>
<tr>
<td>&lt;cr&gt;</td>
<td>You press the &lt;Enter&gt; key to create a line break (carriage return).</td>
</tr>
</tbody>
</table>
User interfaces
1.2 Command Line Interface

The following list displays the possible parameter values within the Command Line Interface:

Table 4: Parameter values in the Command Line Interface

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>This parameter represents a valid IPv4 address. The address consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by a decimal point. The IP address 0.0.0.0 is a valid entry.</td>
</tr>
<tr>
<td>MAC address</td>
<td>This parameter represents a valid MAC address. The address consists of 6 hexadecimal numbers with values from 00 to FF. The numbers are separated by a colon, for example, 00:F6:29:B2:81:40.</td>
</tr>
<tr>
<td>string</td>
<td>User-defined text with a length in the specified range, for example a maximum of 32 characters.</td>
</tr>
<tr>
<td>character string</td>
<td>Use double quotation marks to indicate a character string, for example &quot;System name with space character&quot;.</td>
</tr>
<tr>
<td>number</td>
<td>Whole integer in the specified range, for example 0..999999.</td>
</tr>
<tr>
<td>date</td>
<td>Date in format YYYY-MM-DD.</td>
</tr>
<tr>
<td>time</td>
<td>Time in format HH:MM:SS.</td>
</tr>
</tbody>
</table>

Network addresses

Network addresses are a requirement for establishing a data connection to a remote work station, a server, or another network. You distinguish between IP addresses and MAC addresses.

The IP address is an address allocated by the network administrator. The IP address is unique in one network area.

The MAC addresses are assigned by the hardware manufacturer. MAC addresses are unique worldwide.

The following table displays the representation and the range of the address types:

Table 5: Format and range of network addresses

<table>
<thead>
<tr>
<th>Address Type</th>
<th>Format</th>
<th>Range</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>nnn.nnn.nnn.nnn</td>
<td>nnn: 0 to 255 (decimal)</td>
<td>192.168.11.110</td>
</tr>
<tr>
<td>MAC Address</td>
<td>mm:nn:mm:nn:mm:mm</td>
<td>mm: 00 to ff (hexadecimal number pairs)</td>
<td>A7:C9:89:DD:A9:B3</td>
</tr>
</tbody>
</table>

Strings

A string is indicated by quotation marks. For example, "System name with space character". Space characters are not valid user-defined strings. You enter a space character in a parameter between quotation marks.

Example:

*(GRS)#cli prompt Device name
Error: Invalid command 'name'*

*(GRS)#cli prompt 'Device name'*
1.2.7 Examples of commands

Example 1: clear arp-table-switch

Command for clearing the ARP table of the management agent (cache).

`clear arp-table-switch` is the command name. The command is executable without any other parameters by pressing the <Enter> key.

Example 2: radius server timeout

Command to configure the RADIUS server timeout value.

```
(GRS) (config)#radius server timeout
<1..30> Timeout in seconds (default: 5).
```

`radius server timeout` is the command name.

The parameter is required. The value range is `1..30`.

Example 3: radius server auth modify `<1..8>`

Command to set the parameters for RADIUS authentication server 1.

```
(GRS) (config)#radius server auth modify 1
[name] RADIUS authentication server name.
[msgauth] Enable or disable the message authenticator attribute for this server.
[primary] Configure the primary RADIUS server.
[status] Enable or disable a RADIUS authentication server entry.
[secret] Configure the shared secret for the RADIUS authentication server.
[encrypted] Configure the encrypted shared secret.
<cr> Press Enter to execute the command.
```

`radius server auth modify` is the command name.

The parameter `<1..8>` (RADIUS server index) is required. The value range is `1..8` (integer).

The parameters `[name], [port], [msgauth], [primary], [status], [secret] and [encrypted]` are optional.
1.2.8 Input prompt

Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- (GRS) > User Exec mode
- (GRS) # Privileged Exec mode
- (GRS) (config)# Global Config mode
- (GRS) (Vlan)# VLAN Database mode
- (GRS) ((Interface)all)# Interface Range mode / All ports of the device
- (GRS) ((Interface)2/1)# Interface Range mode / A single port on one interface
- (GRS) ((Interface)1/2-1/4)# Interface Range mode / A range of ports on one interface
- (GRS) ((Interface)1/2,1/4,1/5)# Interface Range mode / A list of single ports
- (GRS) ((Interface)1/1-1/2,1/4-1/6)# Interface Range mode / A list of port ranges and single ports

Asterisk, pound sign and exclamation point

- Asterisk *
  An asterisk * in the first or second position of the input prompt displays you that the settings in the volatile memory and the settings in the non-volatile memory are different. In your configuration, the device has detected modifications which have not been saved.
  *(GRS)>

- Pound sign #
  A pound sign # at the beginning of the input prompt displays you that the boot parameters and the parameters during the boot phase are different.
  *#(GRS)>

- Exclamation point !
  An exclamation point ! at the beginning of the input prompt displays: the password for the admin user account corresponds with the default setting.
  !(GRS)>

Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%d</td>
<td>System date</td>
</tr>
<tr>
<td>%t</td>
<td>System time</td>
</tr>
</tbody>
</table>
1.2 Command Line Interface

The following key combinations make it easier for you to work with the Command Line Interface:

### Table 7: Key combinations in the Command Line Interface

<table>
<thead>
<tr>
<th>Key combination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;H&gt;</code>, <code>&lt;Backspace&gt;</code></td>
<td>Delete previous character</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;A&gt;</code></td>
<td>Go to beginning of line</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;E&gt;</code></td>
<td>Go to end of line</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;F&gt;</code></td>
<td>Go forward one character</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;B&gt;</code></td>
<td>Go backward one character</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;D&gt;</code></td>
<td>Delete current character</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;U&gt;</code>, <code>&lt;X&gt;</code></td>
<td>Delete to beginning of line</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;K&gt;</code></td>
<td>Delete to end of line</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;W&gt;</code></td>
<td>Delete previous word</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;P&gt;</code></td>
<td>Go to previous line in history buffer</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;R&gt;</code></td>
<td>Rewrite or paste the line</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;N&gt;</code></td>
<td>Go to next line in history buffer</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;Z&gt;</code></td>
<td>Return to root command prompt</td>
</tr>
<tr>
<td><code>&lt;CTRL&gt;</code> + <code>&lt;G&gt;</code></td>
<td>Aborts running tcpdump session</td>
</tr>
<tr>
<td><code>&lt;Tab&gt;</code>, <code>&lt;SPACE&gt;</code></td>
<td>Command line completion</td>
</tr>
<tr>
<td><code>Exit</code></td>
<td>Go to next lower command prompt</td>
</tr>
<tr>
<td><code>&lt;?&gt;</code></td>
<td>List choices</td>
</tr>
</tbody>
</table>
The Help command displays the possible key combinations in Command Line Interface on the screen:

(GRS) #help

HELP:
Special keys:

Ctrl-H, BkSp delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-P .... go to previous line in history buffer
Ctrl-R .... rewrites or pastes the line
Ctrl-N .... go to next line in history buffer
Ctrl-Z .... return to root command prompt
Ctrl-G .... aborts running tcpdump session
Tab, <SPACE> command-line completion
Exit .... go to next lower command prompt
? .... list choices

(GRS) #

Figure 8: Listing the key combinations with the Help command
1.2.10 Data entry elements

Command completion

To simplify typing commands, the Command Line Interface lets you use command completion (Tab Completion). Thus you are able to abbreviate key words.

- Type in the beginning of a keyword. When the characters entered identify a keyword, the Command Line Interface completes the keyword after you press the tab key or the space key. When there is more than one option for completion, enter the letter or the letters necessary for uniquely identifying the keyword. Press the tab key or the space key again. After that, the system completes the command or parameter.
- When you make a non-unique entry and press <Tab> or <Space> twice, the Command Line Interface provides you with a list of options.
- On a non-unique entry and pressing <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness. When several commands exist and you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options.

Example:
(GRS) (Config)#lo
(GRS) (Config)#log
logging logout
When you enter lo and <Tab> or <Space>, the Command Line Interface completes the command up to the end of the uniqueness to log.
When you press <Tab> or <Space> again, the Command Line Interface provides you with a list of options (logging logout).

Possible commands/parameters

You can obtain a list of the commands or the possible parameters by entering help or ?, for example by entering (GRS) >show ?

When you enter the command displayed, you get a list of the parameters available for the command show.

When you enter the command without space character in front of the question mark, the device displays the help text for the command itself:

!*#(GRS) (Config)#show?

    show          Display device options and settings.
1.2.11 Use cases

Saving the Configuration

To help ensure that your password settings and your other configuration changes are kept after the device is reset or after an interruption of the voltage supply, you save the configuration. To do this, perform the following steps:

1. Enter `enable` to change to the Privileged Exec mode.
2. Enter the following command:
   ```
   save [profile]
   ```
3. Execute the command by pressing the <Enter> key.

Syntax of the „radius server auth add“ command

Use this command to add a RADIUS authentication server.

- **Mode**: Global Config mode
- **Privilege Level**: Administrator
- **Format**: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `<name>`: RADIUS authentication server name.
  - `<port>`: RADIUS authentication server port (default value: 1813).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1..8&gt;</code></td>
<td>RADIUS server index.</td>
<td>1..8</td>
</tr>
<tr>
<td><code>&lt;a.b.c.d&gt;</code></td>
<td>RADIUS accounting server IP address.</td>
<td>IP address</td>
</tr>
<tr>
<td><code>&lt;string&gt;</code></td>
<td>Enter a user-defined text, max. 32 characters.</td>
<td></td>
</tr>
<tr>
<td><code>&lt;1..65535&gt;</code></td>
<td>Enter port number between 1 and 65535</td>
<td></td>
</tr>
</tbody>
</table>

Mode and Privilege Level:

- The prerequisite for executing the command: You are in the Global Config mode. See “Mode-based command hierarchy” on page 22.
- The prerequisite for executing the command: You have the access role administrator.


Examples for executable commands:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`
### 1.2.12 Service Shell

The Service Shell is for service purposes only.

The Service Shell lets users have access to internal functions of the device. When you need assistance with your device, the service personnel use the Service Shell to monitor internal conditions for example, the switch or CPU registers.

Do not execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the non-volatile memory (NVM) possibly leads to an inoperative device.

### Start the Service Shell

The prerequisite is that you are in User Exec mode: (GRS) >

Perform the following steps:

- Enter `enable` and press the <Enter> key.
  
  To reduce the effort when typing:
  - Enter `e` and press the <Tab> key.

- Enter `serviceshell start` and press the <Enter> key.
  
  To reduce the effort when typing:
  - Enter `ser` and press the <Tab> key.
  - Enter `s` and press the <Tab> key.

```bash
!GRS >enable
!*GRS #serviceshell start
WARNING! The service shell offers advanced diagnostics and functions.
Proceed only when instructed by a service technician.

You can return to the previous mode using the 'exit' command.

BusyBox v1.31.0 (2022-08-25 12:15:23 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

### Working with the Service Shell

When the Service Shell is active, the timeout of the Command Line Interface is inactive. To help prevent configuration inconsistencies, end the Service Shell before any other user starts transferring a new configuration to the device.
Display the Service Shell commands

The prerequisite is that you already started the Service Shell.

Perform the following steps:
- Enter `help` and press the <Enter> key.

```
/mnt/fastpath # help
Built-in commands:
--------------------
. : [ ! ]( alias bg break cd chdir command continue echo eval exec exit export false fg getopts hash help history jobs kill let local pwd read readonly return set shift source test times trap true type ulimit umask unalias unset wait
/mnt/fastpath #
```

End the Service Shell

Perform the following steps:
- Enter `exit` and press the <Enter> key.

Deactivate the Service Shell permanently in the device

When you deactivate the Service Shell, you are still able to configure the device. However, you limit the possibilities of service personnel to perform system diagnostics. The service technician will no longer be able to access internal functions of your device.

The deactivation is irreversible. The Service Shell remains permanently deactivated. In order to reactivate the Service Shell, the device requires disassembly by the manufacturer.

The prerequisites are:
- The Service Shell is not started.
- You are in User Exec mode: `(GRS) >`

Perform the following steps:
- Enter `enable` and press the <Enter> key.
  - To reduce the effort when typing:
    - Enter `e` and press the <Tab> key.
Enter `serviceshell deactivate` and press the <Enter> key.
To reduce the effort when typing:
- Enter `ser` and press the <Tab> key.
- Enter `dea` and press the <Tab> key.

This step is irreversible!
Press the <Y> key.

!GRS >enable

!*GRS #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N)?
1.3 System monitor

The System Monitor lets you set basic operating parameters before starting the operating system.

1.3.1 Functional scope

In the System Monitor, you carry out the following tasks, for example:
- Managing the operating system and verifying the software image
- Starting the operating system
- Deleting configuration profiles, resetting the device to the factory defaults
- Checking boot code information

1.3.2 Starting the System Monitor

You establish a serial connection to the device using the USB-C interface. During the system startup, the serial interface of the device is unavailable. For this reason, starting the System Monitor works differently from other Hirschmann Automation and Control GmbH devices. To start the System Monitor, you set the device to the Recovery Mode.

Set the device to the Recovery Mode

Required accessories:
- External memory (recommended: ACA22-USB-C)
- USB-C to USB-A adapter (only if you use a different external memory than the recommended one)
- USB cable to connect the USB-C port of the device with the computer
- Computer with VT100 terminal emulation (for example PuTTY) or a serial terminal

Perform the following steps:
- Plug the external memory into your computer.
- In the root directory of the external memory, create an empty file named recovery.txt.
- Plug the external memory into the device.
- Reboot the device.
- Observe the LEDs while the device boots. When the Status LED flashes alternately red and green, the device has successfully booted into the Recovery Mode.

Note: You find the description of the display elements in the “Installation” user manual.

Access the System Monitor

Perform the following steps:
- Remove the external memory from the device.
- Connect your computer to the device using the USB cable.
- Open the VT100 terminal emulation on the computer to display the System Monitor.
- Select the appropriate COM port.

When the computer and the device are successfully connected, you see a black screen.
Perform the following steps:

- Press the <Enter> key to display the System Monitor.
  You see the following view on your computer:

```
System Monitor 1
(Selected OS: ...-9.1 (2022-08-23 09:03))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)
```

```
sysMon1>
```

**Figure 9: System Monitor view**

- To select a menu item, enter the corresponding number.
- To leave a submenu and return to the main menu, press the <ESC> key.

**Note:** To boot the device normally next time, only add the external memory without the `recovery.txt` file.
User interfaces
1.3 System monitor
2 Specifying the IP parameters

When you install the device for the first time, specify the IP parameters.

The device provides the following options for entering the IP parameters during the first installation:

- Entry using the Command Line Interface.
  When you preconfigure your device outside its operating environment, or restore the network access ("In-Band") to the device, choose this "Out-of-Band" method.

- Entry using the HiDiscovery protocol.
  When you have a previously installed network device or you have another Ethernet connection between your PC and the device, you choose this "In-Band" method.

- Configuration using the external memory.
  When you are replacing a device with a device of the same type and have already saved the configuration in the external memory, you choose this method.

- Using BOOTP.
  To configure the installed device using BOOTP, you choose this "In-Band" method. You need a BOOTP server for this method. The BOOTP server assigns the configuration data to the device using its MAC address. The DHCP mode is the default mode for the configuration data reference.

- Configuration using DHCP.
  To configure the installed device using DHCP, you choose this "In-Band" method. You need a DHCP server for this method. The DHCP server assigns the configuration data to the device using its MAC address or its system name.

- Configuration using the Graphical User Interface.
  When the device already has an IP address and is reachable using the network, the Graphical User Interface provides you with another option for configuring the IP parameters.

2.1 IP parameter basics

2.1.1 IPv4

IP address

The IP addresses consist of 4 bytes. Write these 4 bytes in decimal notation, separated by a decimal point.

RFC 1340 written in 1992, defines 5 IP Address classes.

Table 8: IP address classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Network address</th>
<th>Host address</th>
<th>Address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1 Byte</td>
<td>3 Bytes</td>
<td>0.0.0.0 to 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>2 Bytes</td>
<td>2 Bytes</td>
<td>128.0.0.0 to 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>3 Bytes</td>
<td>1 Byte</td>
<td>192.0.0.0 to 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td>224.0.0.0 to 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td>240.0.0.0 to 255.255.255.255</td>
</tr>
</tbody>
</table>
The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the IANA ("Internet Assigned Numbers Authority"). When you require an IP address block, contact your Internet Service Provider (ISP). Your ISP contacts their local higher-level organization to reserve an IP address block:

- APNIC (Asia Pacific Network Information Center)
  Asia/Pacific Region
- ARIN (American Registry for Internet Numbers)
  Americas and Sub-Sahara Africa
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens)
  Europe and Surrounding Regions

![Bit representation of the IP address](image)

When the first bit of an IP address is a zero, it belong to class A for example, the first octet is less than 128.

When the first bit of an IP address is a one and the second bit is a zero, it belongs to class B for example, the first octet is between 128 and 191.

When the first 2 bits of an IP address are a one, it belongs to class C for example, the first octet is higher than 191.

Assigning the host address (host ID) is the responsibility of the network operator. The network operator alone is responsible for the uniqueness of the assigned IP addresses.

**Netmask**

Routers and Gateways subdivide large networks into subnetworks. The netmask assigns the IP addresses of the individual devices to a particular subnetwork.

You perform subnetwork division using the netmask in much the same way as the division of the network addresses (net id) into classes A to C.

Set the bits of the host address (host id) that represent the mask to one. Set the remaining host address bits to zero (see the following examples).

**Example of a subnet mask:**

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B
Example of applying the subnet mask to IP addresses for subnetwork assignment:

Decimal notation
129.218.65.17
128 < 129  191 › Class B

Binary notation
10000001.11011010.01000001.00010001

Subnetwork 1
Network address

Decimal notation
129.218.129.17
128 < 129  191 › Class B

Binary notation
10000001.11011010.10000001.00010001

Subnetwork 2
Network address

Example of how the netmask is used

In a large network it is possible that Gateways and routers separate the management agent from its network management station. How does addressing work in such a case?

The network management station “Romeo” wants to send data to the management agent “Juliet”. Romeo knows Juliet’s IP address and also knows that the router “Lorenzo” knows the way to Juliet.

Romeo therefore puts his message in an envelope and writes Juliet’s IP address as the destination address; for the source address he writes his own IP address on the envelope.

Romeo then places this envelope in a second one with Lorenzo's MAC address as the destination and his own MAC address as the source. This process is comparable to going from Layer 3 to Layer 2 of the ISO/OSI base reference model.

Finally, Romeo puts the entire data packet into the mailbox which is comparable to going from Layer 2 to Layer 1, that means to sending the data packet over the Ethernet.
Lorenzo receives the letter, removes the outer envelope and recognizes from the inner envelope that the letter is meant for Juliet. He places the inner envelope in a new outer envelope and searches his address list (the ARP table) for Juliet’s MAC address; he writes her MAC address on the outer envelope as the destination address and his own MAC address as the source address. He then places the entire data packet in the mail box.

Juliet receives the letter and removes the outer envelope. She finds the inner envelope with Romeo’s IP address. Opening the inner envelope and reading its contents corresponds to transferring the message to the higher protocol layers of the ISO/OSI layer model.

Juliet would now like to send a reply to Romeo. She places her reply in an envelope with Romeo’s IP address as destination and her own IP address as source. But where is she to send the answer? For she did not receive Romeo’s MAC address. It was lost, because Lorenzo replaced the outer envelope.

In the MIB, Juliet finds Lorenzo listed under the variable `hmNetGatewayIPAddr` as a means of communicating with Romeo. She therefore puts the envelope with the IP addresses in a further envelope with Lorenzo’s MAC destination address.

The letter now travels back to Romeo through Lorenzo, the same way the first letter traveled from Romeo to Juliet.

**Classless Inter-Domain Routing**

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users. Resulting in an ineffective usage of the available class B addresses.

Class D contains reserved Multicast addresses. Class E is for experimental purposes. A non-participating Gateway ignores experimental datagrams with these destination addresses.

Since 1993, RFC 1519 has been using Classless Inter-Domain Routing (CIDR) to provide a solution. CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you specify the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the netmask. The mask bits equal the number of bits used for the subnet in a given IP address range.

**Example:**

<table>
<thead>
<tr>
<th>IP address, decimal</th>
<th>Network mask, decimal</th>
<th>IP address, binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.112.1</td>
<td>255.255.255.128</td>
<td>11000000 10101000 01110000 00000001</td>
</tr>
<tr>
<td>192.168.112.127</td>
<td>255.255.255.128</td>
<td>11000000 10101000 01110000 01111111</td>
</tr>
</tbody>
</table>

**CIDR notation:** 192.168.112.0/25

---

The term “supernetting” refers to combining a number of class C address ranges. Supernetting lets you subdivide class B address ranges to a fine degree.
2.1.2 IPv6

**IP parameter basics**

The Internet Protocol version 6 (IPv6) is the new version of the Internet Protocol version 4 (IPv4). The need to implement IPv6 was due to the fact that IPv4 addresses are not sufficient in the context of the growing Internet today. The IPv6 protocol is described in RFC 8200.

Some of the differences between IPv6 and IPv4 are:
- Address representation and length
- Absence of the broadcast address type
- Simplified header structure
- Fragmentation performed only by the source host
- Added capabilities for packet flow identification in the network

Both IPv4 and IPv6 protocols can operate at the same time in the device. This is possible with the use of the Dual IP Layer technique, also referred to as Dual Stack.

**Note:** If you want the device to operate only using the IPv4 function, then disable the IPv6 function in the device.

In the device, the IPv6 protocol has the following restrictions:
- You can specify a maximum number of 8 IPv6 unicast addresses as follows:
  - 4 IPv6 addresses using manual configuration
  - 2 IPv6 addresses when the *Auto* radio button is selected
  - 1 IPv6 address using the DHCPv6 server
  - 1 link-local address
- The IPv6 function can be enabled only on the management interface. The total number of configurable IPv6 addresses can be used at the same time on the interface.
- The IPv6 addresses can be used to set the management IP address of the device. Other services where IPv6 addresses can be used include for example, SNTP, SYSLOG, DNS, and LDAP.
Address representation

The IPv6 address consists of 128 bits. It is represented as 8 groups of 4 hexadecimal digits, each group representing 16 bits, further referred to as a hextet. The hextets are separated by colons (:). IPv6 addresses are not case-sensitive and you can write them in either lowercase or uppercase.

In accordance with RFC 4291, the preferred format for an IPv6 address is x:x:x:x:x:x. Each “x” consists of 4 hexadecimal values and represents a hextet. An example of a preferred format of an IPv6 address is shown in the figure below.

As you can see in the figure above, usually an IPv6 address contains many zeros. In order to shorten IPv6 addresses that contain 0 bits, it is necessary to follow 2 writing rules:

- The first rule is to discard the leading zeros in every hextet. This rule is only applied to leading zeros and not to the trailing zeros of a hextet. If the trailing zeros are also discarded, then the resulting address is ambiguous.
- The second rule uses a special syntax to compress the zeros. You can use 2 adjacent colons “::” to replace a string of adjacent hextets that contain only zeros. The “::” sign can be used only one time in an address. If the “::” sign is used more than one time in an address representation, then there can be more than one possible address expanded from that notation.

When the two rules are applied, the result is commonly known as the compressed format.

In the table below you can find 2 examples of how these rules are applied:

<table>
<thead>
<tr>
<th>Table 9: IPv6 address compression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred</td>
</tr>
<tr>
<td>No leading zeros</td>
</tr>
<tr>
<td>Compressed</td>
</tr>
<tr>
<td>Preferred</td>
</tr>
<tr>
<td>No leading zeros</td>
</tr>
<tr>
<td>Compressed</td>
</tr>
</tbody>
</table>
**Prefix length**

Unlike an IPv4 address, an IPv6 address does not use a subnet mask to identify the network portion of an address. Instead, the IPv6 protocol uses the prefix length.

The text representation of IPv6 address prefixes is similar to the way IPv4 address prefixes are written in Classless Inter-Domain Routing (CIDR):

<ipv6-address>/<prefix-length>

The prefix length range is 0..128. The typical IPv6 prefix length for LANs and other types of networks is /64. This means that the network portion of the address is 64 bits in length. The remaining 64 bits represent the Interface ID, similar to the host portion of the IPv4 address.

In the figure below you can find an example of prefix length bits allocation.

<table>
<thead>
<tr>
<th>64 bits prefix length</th>
<th>64 bits interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009:0CB8:0000:0004</td>
<td>0000:0000:0000:0010</td>
</tr>
</tbody>
</table>

**Address types**

The IPv6 address types are described in RFC 4291.

The IPv6 address types are identified by the high-order bits of the address, as in the table below:

<table>
<thead>
<tr>
<th>Table 10: IPv6 address types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address type</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Unspecified</td>
</tr>
<tr>
<td>Loopback</td>
</tr>
<tr>
<td>Multicast</td>
</tr>
<tr>
<td>Link-local Unicast</td>
</tr>
<tr>
<td>Global Unicast</td>
</tr>
</tbody>
</table>

**The Unspecified address**

The IPv6 address with every bit set to 0 is called the Unspecified address, which corresponds to 0.0.0.0 in IPv4. The Unspecified address is used only to indicate the absence of an address. It is typically used as a source address when a unique address is not determined yet.

**Note:** The Unspecified address cannot be assigned to an interface or used as a destination address.
The Loopback address

The unicast address 0:0:0:0:0:0:0:1 is called the Loopback address. The Loopback address can be used by a device to send an IPv6 packet to itself. The Loopback address cannot be assigned to a physical interface.

The Multicast address

IPv6 does not have a broadcast address like IPv4. But there is an IPv6 all-nodes Multicast address that essentially gives the same result.

An IPv6 Multicast address is used to send an IPv6 packet to multiple destinations. The structure of a Multicast address is as follows: The next 4 bits identify the scope of the Multicast address (how far the packet is transmitted):

- The first 8 bits are set to FF.
- The next 4 bits are the lifetime of the address: 0 is permanent and 1 is temporary.
- The next 4 bits identify the scope of the Multicast address, meaning how far the packets are transmitted through the network.

The Link-Local address

The Link-Local address is used to communicate with other devices on the same link. The term “link” refers to a subnet. Routers do not forward packets with link-local source or destination addresses to other links.

Link-local addresses are used to transmit packets on a single link for scopes such as automatic address configuration, neighbor discovery, or when no routers are present. They have the following format:

Table 11: Link-Local Address format

<table>
<thead>
<tr>
<th>10 bits</th>
<th>54 bits</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111111010</td>
<td>0</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

The Link-Local address is always configured and cannot be changed.

The Global Unicast address

A Global Unicast address is globally unique and can be routed over the Internet. This type of addresses are equivalent to public IPv4 addresses. Currently, only Global Unicast addresses with the first three bits of 001 or 2000::/3 are assigned.

A Global Unicast address has 3 parts:
- Global Routing Prefix
- Subnet ID
- Interface ID.

The Global Routing Prefix is the network portion of the address.

The Subnet ID is used by an organization to identify its subnets and it has up to 16 bits in length. The length of the Subnet ID is given by the length of the Global Routing Prefix.
The Interface ID identifies an interface of a particular node. The term Interface ID is used because one host can have multiple interfaces, each having one or more IPv6 addresses.

The general format for IPv6 Global Unicast addresses is represented in the figure below.

![IPv6 Global Unicast address general format](image)

*Figure 13: IPv6 Global Unicast address general format*
2.2 Specifying the IP parameters using the Command Line Interface

2.2.1 IPv4

There are the following methods you enter the IP parameters:

- BOOTP/DHCP
- HiDiscovery protocol
- External memory
- Command Line Interface using the serial connection

Perform the following steps:

- Set up a connection to the device.
  - The start screen appears.

- Deactivate DHCP.
2.2 Specifying the IP parameters using the Command Line Interface

- **Enter the IP parameters.**
  - **Local IP address**
    In the default setting, the local IP address is **0.0.0.0**.
  - **Netmask**
    When you divided your network into subnetworks, and these are identified with a netmask, enter the netmask here. In the default setting, the local netmask is **0.0.0.0**.
  - **IP address of the Gateway.**
    This entry is only required, in cases where the device and the network management station or TFTP server are located in different subnetworks (see on page 43 “Example of how the netmask is used”).
    Specify the IP address of the Gateway between the subnetwork with the device and the path to the network management station.
    In the default setting, the IP address is **0.0.0.0**.

- **Save the configuration specified using** `copy config running-config nvm`.

After entering the IP parameters, you easily configure the device using the Graphical User Interface.

### IPv6

The device lets you specify the IPv6 parameters using the Command Line Interface over the serial interface. Another option to access the Command Line Interface is using a SSH connection with the use of the IPv4 management address.

Perform the following steps:

- **Set up a connection to the device.**
  - The start screen appears.
Enable the IPv6 protocol if the protocol is disabled.

Enter the IPv6 parameters.

- IPv6 address
  - Valid IPv6 address. The IPv6 address is displayed in a compressed format.

- Prefix length
  - Unlike an IPv4 address, the IPv6 address does not use a subnet mask to identify the network part of an address. This role is performed in IPv6 by the prefix length (see on page 47 "Prefix length").

- EUI option function
  - You can use the EUI option function to automatically configure the Interface ID of the IPv6 address. The device uses the MAC address of its interface with the values ff and fe added between byte 3 and byte 4 to generate a 64-bit Interface ID.
  - You can only select this option for IPv6 addresses that have a prefix length equal to 64.

- IPv6 Gateway address
  - The IPv6 Gateway address is the address of a router through which the device accesses other devices outside its own network.
  - You can specify any IPv6 address except loopback and Multicast addresses.
  - In the default setting, the IPv6 Gateway address is ::.

After entering the IPv6 parameters, you easily configure the device using the Graphical User Interface. To use an IPv6 address in a URL, use the following URL syntax: https://<ipv6_address>.
### 2.3 Specifying the IP parameters using HiDiscovery

The HiDiscovery protocol lets you assign IP parameters to the device using the Ethernet.

You easily configure other parameters using the Graphical User Interface.

Perform the following steps:
- Install the HiDiscovery program on your computer.
- Start the HiDiscovery program.

#### Figure 15: HiDiscovery

When HiDiscovery is started, HiDiscovery automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first network interface found for the PC. When your computer has several network cards, you can select the one you desire in the HiDiscovery toolbar.

HiDiscovery displays a line for every device that responds to a HiDiscovery protocol inquiry.

HiDiscovery lets you identify the devices displayed.
- Select a device line.
- To set the LEDs to flashing for the selected device, click the **Signal** button on the tool bar. To stop the flashing, click the **Signal** button again.
- By double-clicking a line, you open a window in which you specify the device name and the IP parameter.

#### Figure 16: HiDiscovery – assigning IP parameters
**Note:** Disable the HiDiscovery function in the device, after you have assigned the IP parameters to the device.

**Note:** Save the settings so that you will still have the entries after a restart.
2.4 Specifying the IP parameters using the Graphical User Interface

2.4.1 IPv4

Perform the following steps:

- Open the Basic Settings > Network > Global dialog. In this dialog you specify the VLAN in which the device management can be accessed and configure the HiDiscovery access.

- In the VLAN ID column you specify the VLAN in which the device management can be accessed over the network.

  Note here that you can only access the device management using ports that are members of the relevant VLAN.

  The MAC address field displays the MAC address of the device with which you access the device over the network.

- In the HiDiscovery protocol v1/v2 frame you specify the settings for accessing the device using the HiDiscovery software.

  The HiDiscovery protocol lets you allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the HiDiscovery software.

- Open the Basic Settings > Network > IPv4 dialog. In this dialog you specify the source from which the device gets its IP parameters after starting.

  - In the Management interface frame you first specify where the device gets its IP parameters from:

    - In the BOOTP mode, the configuration is using a BOOTP or DHCP server on the basis of the MAC address of the device.

    - In the DHCP mode, the configuration is using a DHCP server on the basis of the MAC address or the name of the device.

    - In the Local mode, the device uses the network parameters from the internal device memory.

  Note: When you change the allocation mode of the IP address, the device activates the new mode immediately after you click the ✔ button.

- If required, you enter the IP address, the netmask and the Gateway in the IP parameter frame.

- Save the settings temporarily. To do this, click the ✔ button.
2.4.2 IPv6

Perform the following steps:

- Open the Basic Settings > Network > IPv6 dialog.
- The IPv6 protocol is enabled by default. Verify if the On radio button is selected in the Operation frame.
- In the Configuration frame you specify where the device gets its IPv6 parameters from:
  - If the None radio button is selected, then the device receives its IPv6 parameters manually. You can manually specify a maximum number of 4 IPv6 addresses. You cannot specify loopback, link-local, and Multicast addresses as static IPv6 addresses.
  - If the Auto radio button is selected, then the device receives its IPv6 parameters dynamically for example, with the use of a Router Advertisement Daemon (radvd). The device receives a maximum of 2 IPv6 addresses.
  - If the DHCPv6 radio button is selected, then the device receives its IPv6 parameters from a DHCPv6 server. The device can receive only one IPv6 address from the DHCPv6 server.
  - If the All radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.

  **Note:** When you change the allocation mode of the IPv6 address, the device activates the new mode immediately after you click the ✔ button.

- If necessary, you enter the Gateway address in the IP parameter frame.

  **Note:** If the Auto radio button is selected and you use a Router Advertisement Daemon (radvd), then the device automatically receives a link-local type Gateway address with a higher metric than the manually set Gateway address.

- In the Duplicate Address Detection frame you can specify the number of consecutive Neighbor Solicitation messages that the device sends for the Duplicate Address Detection function (see on page 62 “Duplicate Address Detection”).

  **Note:** When you change the allocation mode of the IPv6 address, the device activates the new mode immediately after you click the ✔ button.

Save the settings temporarily. To do this, click the ✔ button.

Manually specify an IPv6 address. To do this, perform the following steps:

- Open the Basic Settings > Network > IPv6 dialog.
- Click the CREATE button. The dialog displays the Create window.
- Enter the IPv6 address in the IP address field.
- Enter the IPv6 address prefix length in the PrefixLength field.
- Click the Ok button. The device adds a table row.
2.5 Specifying the IP parameters using BOOTP

With the **BOOTP** function activated the device sends a boot request message to the BOOTP server. The boot request message contains the Client ID configured in the **Basic Settings > Network > IPv4** dialog. The BOOTP server enters the Client ID into a database and assigns an IP address. The server answers with a boot reply message. The boot reply message contains the assigned IP address.
2.6 Specifying the IP parameters using DHCP

2.6.1 IPv4

The DHCP (Dynamic Host Configuration Protocol) is a further development of BOOTP, which it has replaced. The DHCP additionally lets the configuration of a DHCP client using a name instead of using the MAC address.

For the DHCP, this name is known as the “Client Identifier” in accordance with RFC 2131.

The device uses the name entered under sysName in the system group of the MIB II as the Client Identifier. You can change the system name using the Graphical User Interface (see dialog Basic Settings > System), the Command Line Interface or SNMP.

The device sends its system name to the DHCP server. The DHCP server then uses the system name to allocate an IP address as an alternative to the MAC address.

In addition to the IP address, the DHCP server sends
- the netmask
- the default Gateway (if available)
- the TFTP URL of the configuration file (if available).

The device applies the configuration data to the appropriate parameters. When the DHCP Sever assigns the IP address, the device permanently saves the configuration data in non-volatile memory.

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subnet Mask</td>
</tr>
<tr>
<td>2</td>
<td>Time Offset</td>
</tr>
<tr>
<td>3</td>
<td>Router</td>
</tr>
<tr>
<td>4</td>
<td>Time server</td>
</tr>
<tr>
<td>12</td>
<td>Host Name</td>
</tr>
<tr>
<td>42</td>
<td>NTP server</td>
</tr>
<tr>
<td>61</td>
<td>Client Identifier</td>
</tr>
<tr>
<td>66</td>
<td>TFTP Server Name</td>
</tr>
<tr>
<td>67</td>
<td>Bootfile Name</td>
</tr>
</tbody>
</table>

The advantage of using DHCP instead of BOOTP is that the DHCP server can restrict the validity of the configuration parameters ("Lease") to a specific time period (known as dynamic address allocation). Before this period ("Lease Duration") elapses, the DHCP client can attempt to renew this lease. Alternatively, the client can negotiate a new lease. The DHCP server then allocates a random free address.

To help avoid this, DHCP servers provide the explicit configuration option of assigning a specific client the same IP address based on a unique hardware ID (known as static address allocation).

In the default setting, DHCP is activated. As long as DHCP is active, the device attempts to obtain an IP address. When the device cannot find a DHCP server after restarting, it will not have an IP address. The Basic Settings > Network > IPv4 dialog lets you activate or deactivate DHCP.
Note: When using Industrial HiVision network management, verify that DHCP allocates the original IP address to every device.

The appendix contains an example configuration of the BOOTP/DHCP-server.

Example of a DHCP-configuration file:

```
# /etc/dhcpd.conf for DHCP Daemon

subnet 10.1.112.0 netmask 255.255.240.0 {
  option subnet-mask 255.255.240.0;
  option routers 10.1.112.96;
}

# Host berta requests IP configuration
# with her MAC address
host berta {
  hardware ethernet 00:80:63:08:65:42;
  fixed-address 10.1.112.82;
}

# Host hugo requests IP configuration
# with his client identifier.
host hugo {
  option dhcp-client-identifier "hugo";
  option dhcp-client-identifier 00:68:75:67:6f;
  fixed-address 10.1.112.83;
  server-name "10.1.112.11";
  filename "/agent/config.dat";
}
```

Lines beginning with the `#` character, contain comments.

The lines preceding the individually listed devices refer to settings that apply to the following device.

The fixed-address line assigns a permanent IP address to the device.

For further information, see the DHCP server manual.

### 2.6.2 IPv6

The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol that is used to dynamically specify IPv6 addresses. This protocol is the IPv6 equivalent of the DHCP protocol for IPv4. DHCPv6 protocol is described in RFC 8415.

The device uses a DHCP Unique Identifier (DUID) to send a request to the DHCPv6 server. In the device, the DUID represents the **Client ID** that the DHCPv6 server uses to identify the device that requested an IPv6 address.

The **Client ID** is displayed in the **Basic Settings > Network > IPv6** dialog, in the **DHCP** frame.

The device can receive only one IPv6 address from the DHCPv6 server, with a **PrefixLength** of 128. No **Gateway address** information is provided. If needed, you can manually specify **Gateway address** information.
In the default setting, DHCPv6 protocol is deactivated. You can activate or deactivate the protocol in the Basic Settings > Network > IPv6 dialog. Verify that the DHCPv6 radio button is selected in the Configuration frame.

If you want to dynamically get an IPv6 address with a PrefixLength other than 128, then select the Auto radio button. An example here is the use of a Router Advertisement Daemon (radvd). The radvd uses Router Solicitation and Router Advertisement messages to automatically configure an IPv6 address.

In the default setting, the Auto radio button is selected. You can select or deselect the Auto radio button in the Basic Settings > Network > IPv6 dialog, in the Configuration frame.

If the All radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.
2.7 Management address conflict detection

You assign an IP address to the device using several different methods. This function helps the device detect IP address conflicts on a network after the system startup and the device also checks periodically during operation. This function is described in RFC 5227.

When enabled, the device sends an SNMP trap informing you that it detected an IP address conflict.

The following list contains the default settings for this function:
- **Operation**: On
- **Detection mode**: active and passive
- **Send periodic ARP probes**: marked
- **Detection delay [ms]**: 200
- **Release delay [s]**: 15
- **Address protections**: 3
- **Protection interval [ms]**: 200
- **Send trap**: marked

2.7.1 Active and passive detection

Actively checking the network helps prevent the device from connecting to the network with a duplicate IP address. After connecting the device to a network or after configuring the IP address, the device immediately checks if its IP address exists within the network. To check the network for address conflicts, the device sends 4 ARP probes with the detection delay of 200 ms into the network. When the IP address exists, the device attempts to return to the previous configuration, and make another check after the configured release delay time.

When you disable active detection, the device sends 2 gratuitous APR announcements in 2 s intervals. Using the ARP announcements with passive detection enabled, the device polls the network to determine if there is an address conflict. After resolving an address conflict or after expired release delay time, the device reconnects to the network. Following 10 detected conflicts, when the configured release delay interval is less than 60 s, the device sets the release delay interval to 60 s.

After the device performs active detection or you disable the active detection function, with passive detection enabled the device listens on the network for other devices using the same IP address. When the device detects a duplicate IP address, it initially defends its address by employing the ACD mechanism in the passive detection mode and sends out gratuitous ARPs. The number of protections that the device sends and the protection interval are configurable. To resolve conflicts, if the remote device remains connected to the network, then the network interface of the local device disconnects from the network.

When a DHCP server assigns an IP address to the device and an address conflict occurs, the device returns a DHCP decline message.

The device uses the ARP probe method. This has the following advantages:
- ARP caches on other devices remain unchanged
- the method is robust through multiple ARP probe transmissions
The **Duplicate Address Detection** function determines the uniqueness of an IPv6 unicast address on an interface. The function is performed when an IPv6 address is configured using manual, **DHCPv6**, or **Auto** methods. The function is also triggered by a change in a link status for example, a link status change from down to up.

The **Duplicate Address Detection** function uses **Neighbor Solicitation** and **Neighbor Advertisement** messages. You have the option to set the number of consecutive **Neighbor Solicitation** messages that the device sends. To do this, perform the following steps:

- **Open the Basic Settings > Network > IPv6 dialog.**
- **In the Duplicate Address Detection frame set the necessary value in the Number of neighbor solicitants field.**
  - Possible values:
    - **0**
      - The function is disabled.
    - **1..5** (default setting: **1**)
- **Save the settings temporarily. To do this, click the **✓** button.**

```
enable
network ipv6 dad-transmits <0..5>
```

To change to the Privileged EXEC mode.
To set the number of **Neighbor Solicitation** messages that the device sends.
The value 0 disables the function.

**Note:** If the **Duplicate Address Detection** function discovers that an IPv6 address is not unique on a link, then the device does not log this event in the log file (System Log).
3 Access to the device

3.1 Access roles

The device functions available to you as a user depend on your access role. When you are logged in with a specific access role, the functions of the access role are available to you.

The commands available to you as a user, also depend on the Command Line Interface mode in which you are currently working. See “Mode-based command hierarchy” on page 22.

The device offers the following access roles:

![Access roles diagram]

Table 13: Access roles and scope of user authorizations

<table>
<thead>
<tr>
<th>Access role</th>
<th>User authorizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest</td>
<td>Users logged in with the access role guest are authorized to monitor the device.</td>
</tr>
<tr>
<td>auditor</td>
<td>Users logged in with the access role auditor are authorized to monitor the device and to save the log file in the Diagnostics &gt; Report &gt; Audit Trail dialog.</td>
</tr>
<tr>
<td>operator</td>
<td>Users logged in with the access role operator are authorized to monitor the device and to change the settings – with the exception of security settings for device access.</td>
</tr>
<tr>
<td>administrator</td>
<td>Users logged in with the access role administrator are authorized to monitor the device and to change the settings.</td>
</tr>
<tr>
<td>unauthorized</td>
<td>Unauthorized users are blocked, and the device rejects the user login. Assign this value to temporarily lock the user account. If a detected error occurs during an access role change, then the device assigns this access role to the user account.</td>
</tr>
</tbody>
</table>
3.2 First login (Password change)

To help prevent undesired access to the device, it is imperative that you change the default password during initial setup.

Perform the following steps:

☐ Open the Graphical User Interface, the HiView application, or the Command Line Interface the first time you log in.

☐ Log in with the default password.

☐ Type in your new password.

To help increase security, choose a password that contains at least 8 characters which includes upper-case characters, lower-case characters, numerical digits, and special characters.

☐ When you log in with the Command Line Interface, the device prompts you to confirm your new password.

☐ Log in again with your new password.

**Note:** If you lost your password, then contact your local support team.

For further information, see hirschmann-support.belden.com.
3.3 Authentication lists

When a user accesses the device using a specific connection, the device verifies the login credentials of the user in an authentication list which contains the policies that the device applies for authentication.

The prerequisite for a user to access the device management is that at least one policy is assigned to the authentication list of the application through which access is performed.

3.3.1 Applications

The device provides an application for each type of connection through which someone accesses the device:

- Access to the Command Line Interface using a serial connection: Console(V.24)
- Access to the Command Line Interface using SSH: SSH
- Access to the Command Line Interface using Telnet: Telnet
- Access to the Graphical User Interface: WebInterface

The device also provides an application to control the access to the network from connected end devices using port-based access control: 8021x

3.3.2 Policies

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users using the following policies:

- User management of the device
- LDAP
- RADIUS

When the end device logs in with valid login data, the device lets the connected end devices have access to the network with the port-based access control according to IEEE 802.1X. The device authenticates the end devices using the following policies:

- RADIUS
- IAS (Integrated Authentication Server)

The device gives you the option of a fall-back solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the current policy, the device applies the next specified policy.

3.3.3 Managing authentication lists

You manage the authentication lists in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

- Open the Device Security > Authentication List dialog.
  The dialog displays the authentication lists that are set up.
3.3 Authentication lists

3.3.4 Adjust the settings

Example: Set up a separate authentication list for the application WebInterface which is by default included in the authentication list defaultLoginAuthList.

The device forwards authentication requests to a RADIUS server in the network. As a fall-back solution, the device authenticates users using the local user management. To do this, perform the following steps:

- Create an authentication list loginGUI.

- Open the Device Security > Authentication List dialog.

- Click the button.

  The dialog displays the Create window.

- Enter a meaningful name in the Name field.
  In this example, enter the name loginGUI.

- Click the Ok button.

  The device adds a table row.

- Select the policies for the authentication list loginGUI.

  - In the Policy 1 column, select the value radius.
  - In the Policy 2 column, select the value local.
  - In the Policy 3 to Policy 5 columns, select the value reject to help prevent further fall-back.

- Save the settings temporarily. To do this, click the ✓ button.
Assign an application to the authentication list loginGUI.

Open the Device Security > Authentication List dialog.
- In the table, select the authentication list loginGUI.
- Click the button.
  - The dialog displays the Allocate applications window.
- Click the application WebInterface to highlight it.
- Click the Ok button.
  - The Dedicated applications column of authentication list loginGUI displays the application WebInterface.
  - The Dedicated applications column of authentication list defaultLoginAuthList does not display the application WebInterface anymore.
- Save the settings temporarily. To do this, click the button.

To display the applications and the allocated lists.

To assign the loginGUI application to the authentication list WebInterface.
3.4 **User management**

When a user logs in with valid login data, the device lets the user have access to its device management. The device authenticates the users either using the local user management or with a RADIUS server in the network. To get the device to use the user management, assign the local policy to an authentication list, see the *Device Security > Authentication List* dialog.

In the local user management, you manage the user accounts. One user account is usually allocated to each user.

3.4.1 **Access roles**

The device lets you use a role-based authorization model to specifically control the access to the device management. Users to whom a specific authorization profile is allocated are allowed to use commands and functions from the same authorization profile or a lower one.

The device uses the authorization profiles on every application with which the device management can be accessed.
Every user account is linked to an access role that regulates the access to the individual functions of the device. Depending on the planned activity for the respective user, you assign a pre-defined access role to the user. The device differentiates between the following access roles.

**Table 14: Access roles for user accounts**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Authorized for the following activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>administrator</strong></td>
<td>The user is authorized to monitor and administer the device.</td>
<td>All activities with read/write access, including the following activities reserved for an administrator:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Add, modify or delete user accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Activate, deactivate or unlock user accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Change every password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Configure password management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Set or change system time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Load files to the device, for example device configurations, certificates or software images</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Reset settings and security-related settings to the state on delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Configure RADIUS server and authentication lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Apply scripts using the Command Line Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Enable/disable CLI logging and SNMP logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► External memory activation and deactivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► System monitor activation and deactivation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Enable/disable the services for the access to the device management (for example SNMP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>► Configure access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses</td>
</tr>
<tr>
<td><strong>operator</strong></td>
<td>The user is authorized to monitor and configure the device - with the exception of security-related settings.</td>
<td>All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:</td>
</tr>
<tr>
<td><strong>auditor</strong></td>
<td>The user is authorized to monitor the device and to save the log file in the Diagnostics &gt; Report &gt; Audit Trail dialog.</td>
<td>Monitoring activities with read access.</td>
</tr>
<tr>
<td><strong>guest</strong></td>
<td>The user is authorized to monitor the device - with the exception of security-related settings.</td>
<td>Monitoring activities with read access.</td>
</tr>
<tr>
<td><strong>unauthorized</strong></td>
<td>No access to the device possible.</td>
<td>No activities allowed.</td>
</tr>
<tr>
<td></td>
<td>As an administrator you assign this access role to temporarily lock a user account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If an administrator assigns a different access role to the user account and an error is detected, then the device assigns this access role to the user account.</td>
<td></td>
</tr>
</tbody>
</table>
3.4.2 Managing user accounts

You manage the user accounts in the Graphical User Interface or in the Command Line Interface. To do this, perform the following steps:

- Open the Device Security > User Management dialog.
  The dialog displays the user accounts that are set up.

3.4.3 Default setting

In the state on delivery, the user account admin is set up in the device.

Table 15: Default settings for the factory setting user accounts

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>private</td>
</tr>
<tr>
<td>Role</td>
<td>administrator</td>
</tr>
<tr>
<td>User locked</td>
<td>unmarked</td>
</tr>
<tr>
<td>Policy check</td>
<td>unmarked</td>
</tr>
<tr>
<td>SNMP auth type</td>
<td>hmacmd5</td>
</tr>
<tr>
<td>SNMP encryption type</td>
<td>des</td>
</tr>
</tbody>
</table>

Change the password for the admin user account before making the device available in the network.

3.4.4 Changing default passwords

To help prevent undesired access, change the password of the default user account. To do this, perform the following steps:

- Change the password for the admin user account.

  - Open the Device Security > User Management dialog.
    The dialog displays the user accounts that are set up.
  
  - To obtain a higher level of complexity for the password, mark the checkbox in the Policy check column.
    Before saving it, the device checks the password according to the policy specified in the Password policy frame.
3.4 User management

3.4.5 Setting up a new user account

Allocate a separate user account to each user that accesses the device management. In this way you can specifically control the authorizations for the access.

In the following example, we will set up the user account for a user **USER** with the access role **operator**. Users with the access role **operator** are authorized to monitor and configure the device - with the exception of security-related settings. To do this, perform the following steps:

1. Create a new user account.
2. Click the table row of the relevant user account in the **Password** field. Enter a password of at least 6 characters.
   Up to 64 alphanumeric characters are allowed.
   - The device differentiates between upper and lower case.
   - The minimum length of the password is specified in the **Configuration** frame. The device constantly checks the minimum length of the password.
3. Save the settings temporarily. To do this, click the ✔ button.

Note: The password check can lead to a message in the **Security status** frame in the **Basic Settings > System** dialog. You specify the settings that cause this message in the **Basic Settings > System** dialog.

- Click the table row of the relevant user account in the **Password** field. Enter a password of at least 6 characters.
  - The device differentiates between upper and lower case.
  - The minimum length of the password is specified in the **Configuration** frame. The device constantly checks the minimum length of the password.
- Save the settings temporarily. To do this, click the ✔ button.

Note: When you display the security status, the password check can lead to a message (**show security-status all**). You specify the settings that cause this message with the command

```
security-status monitor pwd-policy-inactive
```

To specify the password **SECRET** for the **USER** user account. Enter at least 6 characters.

To save the settings in the non-volatile memory (**nvm**) in the “selected” configuration profile.

- Open the **Device Security > User Management** dialog.
- Click the ✔ button.
  - The dialog displays the **Create** window.
- Enter the name in the **User name** field.
  - In this example, we give the user account the name **USER**.
- Click the **Ok** button.
- To obtain a higher level of complexity for the password, mark the checkbox in the **Policy check** column.
  - Before saving it, the device checks the password according to the policy specified in the **Password policy** frame.
3.4 User management

3.4.6 Deactivating the user account

After a user account is deactivated, the device denies the related user access to the device management. In contrast to completely deleting it, deactivating a user account lets you keep the settings and reuse them in the future. To do this, perform the following steps:

- To keep the user account settings and reuse them in the future, you temporarily deactivate the user account.

  - Open the Device Security > User Management dialog.
  - The dialog displays the user accounts that are set up.
  - In the table row for the relevant user account, unmark the checkbox in the Active column.
  - Save the settings temporarily. To do this, click the ✓ button.
To permanently deactivate the user account settings, you delete the user account.

Select the table row of the relevant user account.

Click the button.

To delete the user account .

To display the user accounts that are set up.

To save the settings in the non-volatile memory in the “selected” configuration profile.

3.4.7 Adjusting policies for passwords

The device lets you check if the passwords for the user accounts match the specified policy. When the passwords match the policy, you obtain a higher level of complexity for the passwords.

The user management of the device lets you activate or deactivate the check separately in each user account. When you mark the checkbox and the new password fulfills the requirements of the policy, the device accepts the password change.
In the default settings, practical values for the policy are set up in the device. You have the option of adjusting the policy to meet your requirements. To do this, perform the following steps:

- Adjust the policy for passwords to meet your requirements.

- Open the Device Security > User Management dialog.
  
  In the Configuration frame you specify the number user login attempts before the device locks out the user. You also specify the minimum number of characters that defines a password.

  **Note:** The device lets only users with the administrator authorization remove the lock.

  The number of login attempts as well as the possible lockout of the user apply only when accessing the device management through:
  - the Graphical User Interface
  - the SSH protocol
  - the Telnet protocol

  **Note:** When accessing the device management using the Command Line Interface through the serial connection, the number of login attempts is unlimited.

- Specify the values to meet your requirements.
  
  - In the Login attempts field you specify the number of times that a user attempts to log in. The field lets you define this value in the range 0..5.
    
    In the above example, the value 0 deactivates the function.
  
  - The Min. password length field lets you enter values in the range 1..64.

  The dialog displays the policy set up in the Password policy frame.

- Adjust the values to meet your requirements.
  
  - Values in the range 1 through 16 are allowed.
    
    The value 0 deactivates the relevant policy.

To apply the entries specified in the Configuration and Password policy frames, mark the checkbox in the Policy check column for a particular user.

- Save the settings temporarily. To do this, click the  button.

```
enable
configure
passwords min-length 6
passwords min-lowercase-chars 1
passwords min-numeric-chars 1
passwords min-special-chars 1
passwords min-uppercase-chars 1
show passwords
save
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the policy for the minimum length of the password.
To specify the policy for the minimum number of lower-case letters in the password.
To specify the policy for the minimum number of digits in the password.
To specify the policy for the minimum number of special characters in the password.
To specify the policy for the minimum number of upper-case letters in the password.
To display the policies that are set up.
To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
3.5 LDAP

Server administrators manage Active Directories which contain user login credentials for applications used in the office environment. The Active Directory is hierarchical in nature, containing user names, passwords, and the authorized read/write permission levels for each user.

This device uses the Lightweight Directory Access Protocol (LDAP) to retrieve user login information and permission levels from a Active Directory. This provides a “single sign on” for network devices. Retrieving the login credentials from an Active Directory lets the user log in with the same login credentials used in the office environment.

An LDAP session starts with the device contacting the Directory System Agent (DSA) to search the Active Directory of an LDAP server. If the server finds multiple entries in the Active Directory for a user, then the server sends the higher permission level found. The DSA listens for information requests and sends responses on TCP port 389 for LDAP, or on TCP port 636 for LDAP over SSL (LDAPS). Clients and servers encode LDAPS requests and responses using the Basic Encoding Rules (BER). The device opens a new connection for every request and closes the connection after receiving a response from the server.

The device lets you upload a CA certificate to validate the server for Secure Socket Level (SSL) and Transport Layer Security (TLS) sessions. Whereby, the certificate is optional for TLS sessions.

The device is able to cache login credentials for up to 1024 users in memory. If the active directory servers are unreachable, then the users are still able to log in using their office login credentials.

3.5.1 Coordination with the server administrator

Configuring the LDAP function requires that the network administrator request the following information from the server administrator:

- The server name or IP address
- The location of the Active Directory on the server
- The type of connection used
- The TCP listening port
- When required, the location of the CA certificate
- The name of the attribute containing the user login name
- The names of the attribute containing the user permission levels

The server administrator can assign permission levels individually using an attribute such as description, or to a group using the memberOf attribute. In the Device Security > LDAP > Role Mapping dialog you specify which attributes receive the various permission levels.

You also have the option to retrieve the name of the attributes containing the user login name and permission levels using a LDAP browser such as JXplorer or Softerra.
### 3.5.2 Example configuration

The device is able to establish an encrypted link to a local server using only the server name or to a server on a different network using an IP address. The server administrator uses attributes to identify login credentials of a user and assign individual and group permission levels.

Using information received from the server administrator, specify which attributes in the Active Directory contain the user login credentials and permission level. The device then compares the user login credentials with the permission levels specified in the device and lets the user log in at the assigned permission level.

![Figure 17: LDAP Example Configuration](image)

For this example, the server administrator sent the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Primary Server</th>
<th>Backup Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>The server name or IP address</td>
<td>local.server</td>
<td>10.16.1.2</td>
</tr>
<tr>
<td>The location of the Active Directory on the server</td>
<td>Country/City/User</td>
<td>Country/Company/User</td>
</tr>
<tr>
<td>The type of connection used</td>
<td>TLS (with certificate)</td>
<td>SSL</td>
</tr>
<tr>
<td>The server administrator sent the CA certificate in an email.</td>
<td>CA certificate for primary server saved locally</td>
<td>CA certificate for backup server saved locally</td>
</tr>
<tr>
<td>The TCP listening port</td>
<td>389 (tls)</td>
<td>636 (ssl)</td>
</tr>
<tr>
<td>Name of the attribute containing the user name</td>
<td>userPrincipalName</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>The names of the attribute containing the user permission levels</td>
<td>OPERATOR</td>
<td>OPERATOR</td>
</tr>
<tr>
<td></td>
<td>ADMINISTRATOR</td>
<td>ADMINISTRATOR</td>
</tr>
</tbody>
</table>

Perform the following steps:

- Open the **Device Security > Authentication List** dialog.
- To configure the device to retrieve the user login credentials, during login using the Graphical User Interface, from the Active Directory first, specify for the **defaultLoginAuthList** list the value ldap in the **Policy 1** column.
- Open the **Device Security > LDAP > Configuration** dialog.
- The device lets you specify the length of time that it saves the user login credentials in the cache. To cache user login credentials for a day, in the **Configuration** frame, **Client cache timeout [min]** field, specify the value 1440.
- The **Bind user** entry is optional. When specified, users enter only their user name to log in. The service user can be anyone with login credentials listed in the Active Directory under the attribute specified in the **User name attribute** column. In the **Bind user** column, specify the user name and the domain.
The Base DN is a combination of the domain component (dc) and the organizational unit (ou). The Base DN lets the device locate a server in a domain (dc) and find the Active Directory (ou). Specify the location of the Active Directory. In the Base DN column, specify the value ou=Users,ou=City,ou=Country,dc=server,dc=local.

In the User name attribute column, enter the value userPrincipalName to specify the attribute under which the server administrator lists the users.

The device uses a CA certificate to verify the server.

When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively, click in the area to select the certificate.

To transfer the CA certificate onto the device, click the Start button.

To add a table row, click the button.

To specify a description, enter the value Primary AD Server in the Description column.

To specify the server name and domain of the primary server, in the Address column, enter the value local.server.

The primary server uses the TCP port 389 for communication which is the Destination TCP port default value.

The primary server uses TLS for encrypting communication and a CA certificate for server validation. In the Connection security column, specify the value startTLS.

To activate the table row, mark the checkbox in the Active column.

Using the information received from the server administrator for the Backup server, add, configure and activate another table row.

Open the Device Security > LDAP > Role Mapping dialog.

To add a table row, click the button.

When a user logs in, with LDAP configured and enabled, the device searches the Active Directory for the login credentials of the user. If the device finds the user name and the password is correct, then the device searches for the value specified in the Type column. If the device finds the attribute and the text in the Parameter column matches the text in the Active Directory, then the device lets the user log in with the assigned permission level. When the value attribute is specified in the Type column, specify the value in the Parameter column in the following form: attributeName=attributeValue.

In the Role column, enter the value operator to specify the access role.

To activate the table row, mark the checkbox in the Active column.

Click the button.

The dialog displays the Create window.

Enter the values received from the server administrator for the access role administrator.

To activate the table row, mark the checkbox in the Active column.

Open the Device Security > LDAP > Configuration dialog.

To enable the function, select the On radio button in the Operation frame.
The following table describes how to configure the **LDAP** function in the device using the Command Line Interface. The table displays the commands for **Index 1**. To configure **Index 2**, use the same commands and substitute the appropriate information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td><code>ldap cache-timeout 1440</code></td>
<td>To specify the device to flush the non-volatile memory after a day.</td>
</tr>
<tr>
<td><code>ldap client server add 1 local.server port 389</code></td>
<td>To add a connection to the remote authentication client server with the host name <code>local.server</code> and the UDP port <code>389</code>.</td>
</tr>
<tr>
<td><code>ldap client server modify 1 security startTLS</code></td>
<td>To specify the type of security used for the connection.</td>
</tr>
<tr>
<td><code>ldap client server modify 1 description Primary_AD_Server</code></td>
<td>To specify the configuration name of the entry.</td>
</tr>
<tr>
<td><code>ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local</code></td>
<td>To specify the Base Domain Name used to find the Active Directory on the server.</td>
</tr>
<tr>
<td><code>ldap search-attr userPrincipalName</code></td>
<td>To specify the attribute to search for in the Active Directory which contains the login credential of the users.</td>
</tr>
<tr>
<td><code>ldap bind-user user@company.com</code></td>
<td>To specify the name and domain of the service user.</td>
</tr>
<tr>
<td><code>ldap bind-passwd Ur-123456</code></td>
<td>To specify the password of the service user.</td>
</tr>
<tr>
<td><code>ldap client server enable 1</code></td>
<td>To enable the remote authentication client server connection.</td>
</tr>
<tr>
<td><code>ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR</code></td>
<td>To add a remote authentication role mapping entry for the access role <code>operator</code>. Map the access role <code>operator</code> to the attribute containing the word <code>OPERATOR</code>.</td>
</tr>
<tr>
<td><code>ldap mapping enable 1</code></td>
<td>To enable the remote authentication role mapping entry.</td>
</tr>
<tr>
<td><code>ldap operation</code></td>
<td>To enable the remote authentication function.</td>
</tr>
</tbody>
</table>
3.6 **SNMP access**

The SNMP protocol lets you work with a network management system to monitor the device over the network and change its settings.

### 3.6.1 SNMPv1/v2 access

Using SNMPv1 or SNMPv2 the network management system and the device communicate unencrypted. Every SNMP packet contains the community name in plain text and the IP address of the sender.

The community names `public` for read accesses and `private` for write accesses are preset in the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name have access to the device.

Make undesired access to the device more difficult. To do this, perform the following steps:

- Change the default community names in the device.
- Treat the community names with discretion. Anyone who knows the community name for write access, has the ability to change the settings of the device.
- Specify a different community name for read/write access than for read access.
- Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.
- We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

### 3.6.2 SNMPv3 access

Using SNMPv3 the network management system and the device communicate encrypted. The network management system authenticates itself with the device using the login credentials of a user. The prerequisite for the SNMPv3 access is that in the network management system uses the same settings that are defined in the device.

The device lets you specify the `SNMP auth type` and `SNMP encryption type` parameters individually in each user account.

When you set up a new user account in the device, the parameters are preset so that the network management system Industrial HiVision reaches the device immediately.

The user accounts set up in the device use the same passwords in the Graphical User Interface, in the Command Line Interface, and for SNMPv3.

To adapt the SNMPv3 parameters of the user account settings to the settings in your network management system, perform the following steps:

- Open the **Device Security > User Management** dialog.
- The dialog displays the user accounts that are set up.
Click the table row of the relevant user account in the **SNMP auth type** field. Select the desired setting.

Click the table row of the relevant user account in the **SNMP encryption type** field. Select the desired setting.

Save the settings temporarily. To do this, click the ✔ button.

```
enable
configure
users snmpv3 authentication <user> md5 | sha1
users snmpv3 encryption <user> des | aescfb128 | none
show users
save
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To assign the HMAC-MD5 or HMACSHA protocol for authentication requests to the user account `<user>`.

To assign the DES or AES-128 algorithm to the user account `<user>`.

With this algorithm, the device encrypts authentication requests. The value `none` removes the encryption.

To display the user accounts that have been configured.

To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
3.7 Out-of-Band access

The device comes with a separate port that lets you access the device management out-of-band. When there is a high in-band load on the switching ports, you can still use this separate port to access the device management.

The prerequisite is that you connect the management station directly to the USB port. When you use Microsoft Windows, install the RNDIS driver, where necessary. Once you connect the management station, it can communicate with the device management over a virtual network connection.

In the default setting, you can access the device management through this port using the following IP parameters:
- **IP address**: 192.168.248.100
- **Netmask**: 255.255.255.0

The device lets you access the device management using the following protocols:
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 Specifying the IP parameters

When you connect the management station through the USB port, the device assigns the IP address of the USB network interface, increased by 1, to the management station (192.168.248.101 in the default setting). The device lets you change the IP parameters to adapt the device to the requirements of your environment.

Verify that the IP subnet of this network interface is not overlapping with any subnet connected to another interface of the device:
- Management interface

If the management station accesses the device management through the USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- Open the **Basic Settings > Out-of-Band over USB** dialog.
- Overwrite the IP address in the **IP parameter** frame, **IP address** field.
- Save the settings temporarily. To do this, click the **✓** button.
3.7.2 Disable the USB network interface

In the default setting, the USB network interface is enabled. If you do not want someone to access device management through the USB port, then the device lets you disable the USB network interface.

If the management station accesses the device management through the USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- Open the Basic Settings > Out-of-Band over USB dialog.
- To disable the USB network interface, select the Off radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
network usb parms 192.168.1.1
255.255.255.0

show network usb
Out-of-band USB management settings
-----------------------------
Management operation...........enabled
IP address......................192.168.1.1
Subnet mask....................255.255.255.0
Host MAC address...............64:60:38:1f:85:85
Device MAC address............64:60:38:1f:85:86

save
```

To change to the Privileged EXEC mode.
To specify the IP address 192.168.1.1 and the netmask 255.255.255.0 for the USB network interface.
To display the USB network interface settings.

```
To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
```

```
no network usb operation

Out-of-band USB management settings
-----------------------------
Management operation...........disabled
IP address......................192.168.1.1
Subnet mask....................255.255.255.0
Host MAC address...............64:60:38:1f:85:85
Device MAC address............64:60:38:1f:85:86

save
```

To disable the USB network interface.
4 Synchronizing the system time in the network

Many applications rely on a time that is as correct as possible. The necessary accuracy, and thus the allowable deviation from the actual time, depends on the application area.

Examples of application areas include:
- Log entries
- Time stamping of production data
- Process control

The device lets you synchronize the time on the network using the following options:
- The Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, SNTP achieves an accuracy in the millisecond range. The accuracy depends on the signal delay.

When the involved devices support the PTP protocol, it is the better choice. PTP is more accurate, has advanced methods of error correction, and causes a low network load. The implementation of PTP is comparatively easy.

Note: According to the PTP and SNTP standards, both protocols function in parallel in the same network. However, since both protocols influence the system time of the device, situations can occur in which the two protocols conflict with each other.

4.1 Basic settings

In the Time > Basic Settings dialog, you specify general settings for the time.

4.1.1 Setting the time

When no reference time source is available to you, you have the option to set the time in the device.

After a cold start or reboot, if no real-time clock is available or the real-time clock contains an invalid time, then the device initializes its clock with January 1, 00:00h. After the power supply is switched off, the device buffers the settings of the real-time clock up to 24 hours.

Alternatively, you configure the settings in the device so that it automatically obtains the current time from an SNTP server.
Perform the following steps:

- Open the **Time > Basic Settings** dialog.
  - The **System time (UTC)** field displays the current UTC (Universal Time Coordinated) of the device. UTC is the time relating to the coordinated world time measurement. UTC is the same worldwide and does not take local time shifts into account.
  - The time in the **System time** field comes from the **System time (UTC)** plus the **Local offset [min]** value and a possible shift due to daylight saving time.

- In order to cause the device to apply the time of your PC to the **System time** field, click the **Set time from PC** button.
  - Based on the value in the **Local offset [min]** field, the device calculates the time in the **System time (UTC)** field: The **System time (UTC)** comes from the **System time** minus the **Local offset [min]** value and a possible shift due to daylight saving time.

- The **Time source** field displays the origin of the time data. The device automatically selects the source with the greatest accuracy. The source is initially **local**. When SNTP is active and the device receives a valid SNTP packet, the device sets its time source to **sntp**.

- The **Local offset [min]** value specifies the time difference between the local time and the **System time (UTC)**.

- In order to cause the device to determine the time zone on your PC, click the **Set time from PC** button. The device calculates the local time difference from UTC and enters the difference into the **Local offset [min]** field.

**Note:** The device provides the option to obtain the local offset from a DHCP server.

- Save the settings temporarily. To do this, click the **✔️** button.

---

**Enable**
- **configure**
- **clock set <YYYY-MM-DD> <HH:MM:SS>**
- **clock timezone offset <-780..840>**
- **save**

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To set the system time of the device.
To enter the time difference between the local time and the received UTC time in minutes.
To save the settings in the non-volatile memory (**nvm**) in the “selected” configuration profile.
4.1.2 Automatic daylight saving time changeover

When you operate the device in a time zone in which there is a summer time change, you set up the automatic daylight saving time changeover on the Daylight saving time tab.

When daylight saving time is enabled, the device sets the local system time forward by 1 hour at the beginning of daylight saving time. At the end of daylight saving time, the device sets the local system time back again by 1 hour. To do this, perform the following steps:

- Open the Time > Basic Settings dialog, Daylight saving time tab.
- To select a preset profile for the start and end of daylight saving time, click the Profile... button in the Operation frame.
- When no matching daylight saving time profile is available, you specify the changeover times in the Summertime begin and Summertime end fields. For both time points, you specify the month, the week within this month, the weekday, and the time of day.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
clock summer-time mode <disable|recurring|eu|usa>
clock summer-time recurring start
clock summer-time recurring end
save
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To configure the automatic daylight saving time changeover: enable/disable or activate with a profile.
To enter the start time for the changeover.
To enter the end time for the changeover.
To save the settings in the non-volatile memory (nvm) in the "selected" configuration profile.
4.2 SNTP

The Simple Network Time Protocol (SNTP) lets you synchronize the system time in your network. The device supports the SNTP client and the SNTP server function.

The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The UTC is the same worldwide and ignores local time shifts.

SNTP is a simplified version of NTP (Network Time Protocol). The data packets are identical with SNTP and NTP. Accordingly, both NTP and SNTP servers serve as a time source for SNTP clients.

Note: Statements in this chapter relating to external SNTP servers also apply to NTP servers.

SNTP knows the following operation modes for the transmission of time:

- **Unicast**
  - In Unicast operation mode, an SNTP client sends requests to an SNTP server and expects a response from this server.

- **Broadcast**
  - In Broadcast operation mode, an SNTP server sends SNTP messages to the network in specified intervals. SNTP clients receive these SNTP messages and evaluate them.

In an IPv6 environment, the Broadcast operation mode operates as follows:

- The SNTP client listens only for SNTP server messages that have the IPv6 Multicast address set to `ff05::101` as the IPv6 destination address.
- The SNTP server sends only SNTP messages to the Multicast address `ff05::101`. The SNTP server does not send SNTP messages with the link-local address as the IPv6 source address.

<table>
<thead>
<tr>
<th>IPv4 destination address</th>
<th>Send SNTP packets to</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Nobody</td>
</tr>
<tr>
<td>224.0.1.1</td>
<td>Multicast address for SNTP messages</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>Broadcast address</td>
</tr>
</tbody>
</table>

Note: An SNTP server in Broadcast operation mode also responds to direct requests using Unicast from SNTP clients. In contrast, SNTP clients work in either Unicast or Broadcast operation mode.
4.2.1 Preparation

Perform the following steps:

- To get an overview of how the time is passed on, draw a network plan with the devices participating in SNTP.

When planning, bear in mind that the accuracy of the time depends on the delays of the SNTP messages. To minimize delays and their variance, place an SNTP server in each network segment. Each of these SNTP servers synchronizes its own system time as an SNTP client with its parent SNTP server (SNTP cascade). The highest SNTP server in the SNTP cascade has the most direct access to a reference time source.

![Figure 18: Example of SNTP cascade](image-url)
### 4.2 SNTP

**Note:** For precise time distribution, between SNTP servers and SNTP clients you preferably use network components (routers and switches) that forward the SNTP packets with a low and uniform transmission time (latency).

An SNTP client sends its requests to up to 4 configured SNTP servers. When there is no response from the 1st SNTP server, the SNTP client sends its requests to the 2nd SNTP server. When this request is also unsuccessful, it sends the request to the 3rd and finally the 4th SNTP server. If none of these SNTP servers respond, the SNTP client loses its synchronization. The SNTP client periodically sends requests to each SNTP server until a server delivers a valid time.

**Note:** The device provides the option of obtaining a list of SNTP server IP addresses from a DHCP server.

- If no reference time source is available to you, then determine a device with an SNTP server as a reference time source. Adjust its system time at regular intervals.

#### 4.2.2 Defining settings of the SNTP client

As an SNTP client, the device obtains the time information from SNTP or NTP servers and synchronizes its system clock accordingly. To do this, perform the following steps:

- Open the **Time > SNTP > Client** dialog.
- Set the SNTP operation mode.
  - In the **Configuration** frame, select one of the following values in the **Mode** field:
    - **unicast**: The device sends requests to an SNTP server and expects a response from this server.
    - **broadcast**: The device waits for **Broadcast** or **Multicast** messages from SNTP servers on the network.
- To synchronize the time only once, mark the **Disable client after successful sync** checkbox. After synchronization, the device disables the **Client** function.
- The table displays the SNTP server to which the SNTP client sends a request in **Unicast** operation mode. The table contains up to 4 SNTP server definitions.
- To add a table row, click the **+** button.
- To specify the connection data of the SNTP server.
- To enable the function, select the **On** radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the **✓** button.
- The **State** field displays the current status of the **Client** function.

**Table 17: SNTP client settings for the example**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client function</strong></td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td><strong>Configuration: Mode</strong></td>
<td>unicast</td>
<td>unicast</td>
<td>unicast</td>
<td>unicast</td>
<td>unicast</td>
</tr>
<tr>
<td><strong>Request interval [s]</strong></td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td><strong>Server address(es)</strong></td>
<td>–</td>
<td>192.168.1.1</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>192.168.1.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.1.1</td>
<td>192.168.1.2</td>
<td>192.168.1.3</td>
<td>192.168.1.12</td>
</tr>
</tbody>
</table>
4.2.3 Specifying SNTP server settings

When the device operates as an SNTP server, it provides its system time in coordinated world time (UTC) in the network. To do this, perform the following steps:

- Open the Time > SNTP > Server dialog.
- To enable the function, select the On radio button in the Operation frame.
- To enable the Broadcast operation mode, select the Broadcast admin mode radio button in the Configuration frame.
  In Broadcast operation mode, the SNTP server sends SNTP messages to the network in specified intervals. The SNTP server also responds to the requests from SNTP clients in Unicast operation mode.
- In the Broadcast destination address field, you set the IPv4 address to which the SNTP server sends the SNTP packets. Set a Broadcast address or a Multicast address.
  In an IPv6 environment, you cannot set the IPv4 address to which the SNTP server sends the SNTP packets. The SNTP server uses the Multicast address ff05::101 as the IPv6 destination address.
- In the Broadcast UDP port field, you specify the number of the UDP port to which the SNTP server sends the SNTP packets in Broadcast operation mode.
- In the Broadcast VLAN ID field, you specify the ID of the VLAN to which the SNTP server sends the SNTP packets in Broadcast operation mode.
- In the Broadcast send interval [s] field, you specify the time interval at which the SNTP server of the device sends SNTP Broadcast packets.

Note: Except for the Broadcast destination address field, the remaining settings are applicable for both IPv4 and IPv6 SNTP servers.

- Save the settings temporarily. To do this, click the ✓ button.
  The State field displays the current status of the Server function.

Table 18: Settings for the example

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server function</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>UDP port</td>
<td>123</td>
<td>123</td>
<td>123</td>
<td>123</td>
<td>123</td>
</tr>
<tr>
<td>Broadcast admin mode</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
</tr>
<tr>
<td>Broadcast destination address</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Broadcast UDP port</td>
<td>123</td>
<td>123</td>
<td>123</td>
<td>123</td>
<td>123</td>
</tr>
<tr>
<td>Broadcast VLAN ID</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Broadcast send interval [s]</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Disable server at local time source</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
<td>unmarked</td>
</tr>
</tbody>
</table>
Synchronizing the system time in the network

4.2 SNTP
5 Managing configuration profiles

If you change the settings of the device during operation, then the device stores the changes in its memory (RAM). After a reboot the settings are lost.

In order to keep the changes after a reboot, the device lets you save the settings in a configuration profile in the non-volatile memory (NVM). In order to make it possible to quickly switch to other settings, the non-volatile memory offers storage space for multiple configuration profiles.

If an external memory is connected, then the device automatically saves a copy of the configuration profile in the external memory (ENVM). You can disable this function.

5.1 Detecting changed settings

The device stores changes made to settings during operation in its volatile memory (RAM). The configuration profile in the non-volatile memory (NVM) remains unchanged until you save the changed settings explicitly. Until then, the configuration profiles in memory and non-volatile memory are different. The device helps you recognize changed settings.

5.1.1 Volatile memory (RAM) and non-volatile memory (NVM)

You can recognize if the settings in the volatile memory (RAM) differ from the settings of the "selected" configuration profile in the non-volatile memory (NVM). To do this, perform the following steps:

- Check the banner of the Graphical User Interface:
  - When the icon is visible, the settings differ.
  - When no icon is visible, the settings match.

  Or:

- Open the Basic Settings > Load/Save dialog.
- Check the status of the checkbox in the Information frame:
  - When the checkbox is marked, the settings match.
  - When the checkbox is unmarked, the settings differ.

  show config status
  Configuration Storage sync State
  --------------------------------
  running-config to NV..................out of sync
  ...

...
5.1.2 External memory (ACA) and non-volatile memory (NVM)

You can recognize if the settings copied to the external memory (ACA) differ from the settings of the configuration profile in the non-volatile memory (NVM). To do this, perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Check the status of the checkbox in the Information frame:
  - When the checkbox is marked, the settings match.
  - When the checkbox is unmarked, the settings differ.

```
show config status
Configuration Storage sync State
---------------------------
...                         
NV to ACA..............................out of sync
...                         
```
5.2  Saving the settings

5.2.1  Saving the configuration profile in the device

If you change the settings of the device during operation, then the device stores the changes in its memory (RAM). In order to keep the changes after a reboot, save the configuration profile in the non-volatile memory (NVM).

**Saving a configuration profile**

The device stores the settings in the "selected" configuration profile in the non-volatile memory (NVM).

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Verify that the required configuration profile is "Selected".
  You can recognize the "selected" configuration profile because the checkbox in the Selected column is marked.
- Click the button.

**Copying settings to a configuration profile**

The device lets you store the settings saved in the memory (RAM) in a configuration profile other than the "selected" configuration profile. In this way you create a new configuration profile in the non-volatile memory (NVM) or overwrite an existing one.

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Click the button and then the Save as.. item.
  The dialog displays the Save as.. window.
- In the Name field, change the name of the configuration profile. If you keep the proposed name, the device will overwrite an existing configuration profile of the same name.
- Click the Ok button.
  The new configuration profile is designated as “Selected”.

show config profiles nvm
enable
save

To display the configuration profiles contained in the non-volatile memory (nvm).
To change to the Privileged EXEC mode.
To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
5.2 Saving the settings

Selecting a configuration profile

When the non-volatile memory (NVM) contains multiple configuration profiles, you have the option to select any configuration profile there. The device stores the settings in the “selected” configuration profile. During the system startup, the device loads the settings of the “selected” configuration profile into the memory (RAM).

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- The table displays the configuration profiles present in the device. You can recognize the “selected” configuration profile because the checkbox in the Selected column is marked.
- Select the table row of the desired configuration profile stored in the non-volatile memory (NVM).
- Click the  button and then the Select item.
- In the Selected column, the checkbox of the configuration profile is now marked.

To display the configuration profiles contained in the non-volatile memory (nvm).
To change to the Privileged EXEC mode.
To save the current settings in the configuration profile named <string> in the non-volatile memory (nvm). If present, the device overwrites a configuration profile of the same name. The new configuration profile is designated as “Selected”.

To change to the Privileged EXEC mode.
To display the configuration profiles contained in the non-volatile memory (nvm).
To change to the Configuration mode.
To select the configuration profile.
Take note of the adjacent name of the configuration profile.
To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
5.2.2 Saving the configuration profile in the external memory

When an external memory is connected and you save a configuration profile, the device automatically saves a copy in the *Selected external memory*. In the default setting, the function is enabled. You can disable this function.

Perform the following steps:

- Open the *Basic Settings > External Memory* dialog.
- Mark the checkbox in the *Backup config when saving* column in order to enable the device to automatically save a copy in the external memory during the saving process.
- To deactivate the function, unmark the checkbox in the *Backup config when saving* column.
- Save the settings temporarily. To do this, click the ☑ button.

```
enable
configure
config envm config-save usb
save
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To enable the function.
When you save a configuration profile, the device saves a copy in the external memory.
usb = External USB memory
To save the settings in the non-volatile memory (*nvm*) in the “selected” configuration profile.

5.2.3 Backup the configuration profile on a remote server

The device lets you automatically backup the configuration profile to a remote server. The prerequisite is that you activate the function before you save the configuration profile.

After you save the configuration profile in the non-volatile memory (*nvm*), the device sends a copy to the specified URL.

Perform the following steps:

- Open the *Basic Settings > Load/Save* dialog.
- In the *Backup config on a remote server when saving* frame, perform the following steps:
- In the *URL* field, specify the server as well as the path and file name of the backed up configuration profile.
- Click the *Set credentials* button.
The dialog displays the *Credentials* window.
- Enter the login credentials needed to authenticate on the remote server.
- In the *Operation* option list, enable the function.
- Save the settings temporarily. To do this, click the ☑ button.
Managing configuration profiles
5.2 Saving the settings

If the transfer to the remote server is unsuccessful, then the device logs this event in the log file (System Log).

5.2.4 Exporting a configuration profile

The device lets you save a configuration profile to a server as an XML file. If you use the Graphical User Interface, then you have the option to save the XML file directly to your PC.

Prerequisites:
- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password for accessing this server.

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Select the table row of the desired configuration profile.

Export the configuration profile to your PC. To do this, perform the following steps:

- Click the link in the Profile name column.
  The configuration profile is downloaded and saved as an XML file on your PC.
Export the configuration profile to a remote server. To do this, perform the following steps:

- Click the button and then the Export... item. The dialog displays the Export... window.
- In the URL field, specify the file URL on the remote server:
  - To save the file on an FTP server, specify the URL in the following form:
    ftp://<user>:<password>@<IP address>:<port>/<file name>
  - To save the file on a TFTP server, specify the URL in the following form:
    tftp://<IP address>/<path>/<file name>
  - To save the file on an SCP or SFTP server, specify the URL in one of the following forms:
    scp://<user>:<password>@<IP address>/<path>/<file name>
    sftp://<IP address>/<path>/<file name>
  - When you click the Ok button, the device displays the Credentials window. There you enter User name and Password to log in to the server.
  - Click the Ok button.
  The configuration profile is now saved as an XML file in the specified location.

```
show config profiles nvm

enable
copy config running-config remote tftp://<IP_address>/ <path>/<file_name>
copy config nvm remote sftp://<user_name>:<password>@<IP_address>/ <path>/<file_name>
copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>
copy config nvm profile config3 remote ftp://<IP_address>:<port>/ <path>/<file_name>
```

To display the configuration profiles contained in the non-volatile memory (nvm).
To change to the Privileged EXEC mode.
To save the current settings on a TFTP server.
To save the selected configuration profile in the non-volatile memory (nvm) on a SFTP server.
To save the configuration profile config3 in the non-volatile memory (nvm) on a TFTP server.
To save the configuration profile config3 in the non-volatile memory (nvm) on an FTP server.
5.3 Loading settings

If you save multiple configuration profiles in the memory, then you have the option to load a different configuration profile.

5.3.1 Activating a configuration profile

The non-volatile memory of the device can contain multiple configuration profiles. If you activate a configuration profile stored in the non-volatile memory (NVM), then you immediately change the settings in the device. The device does not require a reboot.

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Select the table row of the desired configuration profile.
- Click the button and then the Activate item.

The device copies the settings to the memory (RAM) and disconnects from the Graphical User Interface. The device immediately uses the settings of the configuration profile.

- Reload the Graphical User Interface.
- Log in again.

In the Selected column, the checkbox of the configuration profile that was activated before is marked.

- show config profiles nvm
- enable
- copy config nvm profile config3 running-config

To display the configuration profiles contained in the non-volatile memory (nvm).

To change to the Privileged EXEC mode.

To activate the settings of the configuration profile config3 in the non-volatile memory (nvm). The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the configuration profile config3.

5.3.2 Loading the configuration profile from the external memory

If an external memory is connected, then the device loads a configuration profile from the external memory during the system startup automatically. The device lets you save these settings in a configuration profile in non-volatile memory.

When the external memory contains the configuration profile of an identical device, you have the possibility to transfer the settings from one device to another.
Perform the following steps:

- Verify that the device loads a configuration profile from the external memory during the system startup.
  
  In the default setting, the function is enabled. If the function is disabled, enable it again as follows:
  
  - Open the Basic Settings > External Memory dialog.
  - In the Config priority column, select the value first.
  - Save the settings temporarily. To do this, click the button.

<table>
<thead>
<tr>
<th>enable</th>
<th>To change to the Privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>config envm load-priority usb first</td>
<td>To enable the function.</td>
</tr>
<tr>
<td>During the system startup, the device loads a configuration profile from the external memory. usb = External USB memory</td>
<td></td>
</tr>
</tbody>
</table>

| show config envm settings | To display the settings of the external memory (envm). |

<table>
<thead>
<tr>
<th>Type</th>
<th>Status</th>
<th>Auto Update</th>
<th>Save Config</th>
<th>Config Load Prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>usb</td>
<td>ok</td>
<td>[x]</td>
<td>[x]</td>
<td>first</td>
</tr>
<tr>
<td>save</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using the Command Line Interface, the device lets you copy the settings from the external memory directly into the non-volatile memory (nvm).

<table>
<thead>
<tr>
<th>show config profiles nvm</th>
<th>To display the configuration profiles contained in the non-volatile memory (nvm).</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>copy config envm profile config3 nvm</td>
<td>To copy the configuration profile config3 from the external memory (envm) to the non-volatile memory (nvm).</td>
</tr>
</tbody>
</table>

The device can also automatically load a configuration profile from a script file during the system startup.

Prerequisites:

- Verify that the external memory is connected before you start the device.
- The root directory of the external memory contains a text file startup.txt with the content script=<file_name>. The placeholder <file_name> represents the script file that the device executes during the system startup.
- The root directory of the external memory contains the script file. You have the option to save the script with a user-specified name. Save the file with the file extension .cli.

Note: Verify that the script saved in the external memory is not empty. If the script is empty, then the device loads the next configuration profile as per the configuration priority settings.
After applying the script, the device automatically saves the configuration profile from the script file as an XML file in the external memory. When you type the appropriate command into the script file, you have the option to disable this function:

- `no config envm config-save usb`
  The device does not create a copy in the external USB memory.

When the script file contains an incorrect command, the device does not apply this command during the system startup. The device logs the event in the log file (System Log).

### 5.3.3 Importing a configuration profile

The device lets you import from a server a configuration profile saved as an XML file. If you use the Graphical User Interface, then you can import the XML file directly from your PC.

**Prerequisites:**

- To save the file on a server, you need a configured server on the network.
- To save the file to an SCP or SFTP server, you also need the user name and password for accessing this server.

Perform the following steps:

1. Open the *Basic Settings > Load/Save* dialog.
2. Click the button and then the *Import...* item.
   The dialog displays the *Import...* window.
3. From the *Select source* drop-down list, select the location from where the device imports the configuration profile.
   - *PC/URL*
     The device imports the configuration profile from the local PC or from a remote server.
   - *External memory*
     The device imports the configuration profile from the external memory.
Import the configuration profile from the local PC or from a remote server. To do this, perform the following steps:

- Import the configuration profile:
  - When the file is located on an FTP server, specify the URL for the file in the following form:
    \[ ftp://<user>:<password>@<IP address>:<port>/<file name> \]
  - When the file is located on a TFTP server, specify the URL for the file in the following form:
    \[ tftp://<IP address>/<path>/<file name> \]
  - When the file is located on an SCP or SFTP server, specify the URL for the file in one of the following forms:
    \[ scp://<IP address>/<path>/<file name> \]
    \[ sftp://<IP address>/<path>/<file name> \]
  - When you click the Start button, the device displays the Credentials window. There you enter User name and Password to log in to the server.
  - scp:// or sftp://<user>:<password>@<IP address>/<path>/<file name>

- In the Destination frame, specify where the device saves the imported configuration profile:
  - In the Profile name field, specify the name under which the device saves the configuration profile.
  - In the Storage type field, specify the storage location for the configuration profile.

- Click the Ok button.

  The device copies the configuration profile into the specified memory.

If you specified the value \texttt{ram} in the Destination frame, then the device disconnects the Graphical User Interface and uses the settings immediately.

Import the configuration profile from the external memory. To do this, perform the following steps:

- In the Import profile from external memory frame, select the name of the configuration profile to be imported from the Profile name drop-down list.
  - The prerequisite is that the external memory contains an exported configuration profile.

- In the Destination frame, specify where the device saves the imported configuration profile:
  - In the Profile name field, specify the name under which the device saves the configuration profile.

- Click the Ok button.

  The device copies the configuration profile into the non-volatile memory (NVM) of the device.

If you specified the value \texttt{ram} in the Destination frame, then the device disconnects the Graphical User Interface and uses the settings immediately.
Managing configuration profiles

5.3 Loading settings

enable

*copy config remote ftp://<IP_address>:<port>/<path>/<file_name>*

To change to the Privileged EXEC mode.

running-config

To import and activate the settings of a configuration profile saved on an FTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.

*copy config remote tftp://<IP_address>/ <path>/<file_name>*

To import and activate the settings of a configuration profile saved on a TFTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.

*copy config remote sftp://<user name>:<password>@<IP_address>/ <path>/<file_name>* running-config

To import and activate the settings of a configuration profile saved on a SFTP server. The device copies the settings into the volatile memory and disconnects the connection to the Command Line Interface. The device immediately uses the settings of the imported configuration profile.

*copy config remote ftp://<IP_address>:<port>/<path>/<file_name>*

To import the settings of a configuration profile saved on an FTP server and save the settings in the configuration profile `config3` in the non-volatile memory (nvm).

nvm profile config3

*copy config remote tftp://<IP_address>/ <path>/<file_name>*

To import the settings of a configuration profile saved on a TFTP server and save the settings in the configuration profile `config3` in the non-volatile memory (nvm).

nvm profile config3

Note: Upgrading from Classic to HiOS? Convert your device configuration files using our online tool: https://convert.hirschmann.com
5.4 Reset the device to the factory defaults

If you reset the settings in the device to the delivery state, then the device deletes the configuration profiles in the volatile memory and in the non-volatile memory.

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

The device then reboots and loads the factory settings.

5.4.1 Using the Graphical User Interface or Command Line Interface

Perform the following steps:

- Open the Basic Settings > Load/Save dialog.
- Click the button, then Back to factory.... The dialog displays a message.
- Click the Ok button.

The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM).

If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

After a brief period, the device restarts and loads the delivery settings.

5.4.2 Using the System Monitor

Prerequisite:
- Your PC is connected with the serial connection of the device using a terminal cable.

Perform the following steps:
- Restart the device.
- To change to the System Monitor, press the <1> key within 3 seconds when prompted during reboot.
  The device loads the System Monitor.
- To change from the main menu to the Manage configurations menu, press the <4> key.
- To execute the Clear configs and boot params command, press the <1> key.
To load the factory settings, press the <Enter> key. The device deletes the configuration profiles in the memory (RAM) and in the non-volatile memory (NVM). If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.

To change to the main menu, press the <q> key.
To reboot the device with factory settings, press the <q> key.
6 Loading software updates

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at www.hirschmann.com.

The device gives you the following options for updating the device software:

- Loading a previous software version
- Software update from the PC
- Software update from a server
- Software update from the external memory

Note: The device settings are kept after updating the device software.

You see the version of the installed device software in the login dialog of the Graphical User Interface.

To display the version of the installed software when you are already logged in, perform the following steps:

- Open the Basic Settings > Software dialog.
  - The Running version field displays the version number and creation date of the device software that the device loaded during the last system startup and is currently running.

- enable
- show system info

To change to the Privileged EXEC mode.
To display the system information such as the version number and creation date of the device software that the device loaded during the last system startup and is currently running.

6.1 Loading a previous software version

The device lets you replace the device software with a previous version. The basic settings in the device are kept after replacing the device software.

Note: Only the settings for functions which are available in the newer device software version are lost.
6.2 Software update from the PC

The prerequisite is that the image file of the device software is saved on a data carrier which is accessible from your PC.

Perform the following steps:

- Navigate to the folder where the image file of the device software is saved.
- Open the Basic Settings > Software dialog.
- Drag and drop the image file in the area. Alternatively click in the area to select the file.
- To start the update procedure, click the Start button.

As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated. During the next system startup, the device loads the installed device software.
6.3 Software update from a server

To update the software using SFTP or SCP you need a server on which the image file of the device software is saved.

To update the software using TFTP, SFTP or SCP you need a server on which the image file of the device software is saved.

Perform the following steps:

- Open the Basic Settings > Software dialog.
- In the Software update frame, URL field, enter the URL for the image file in the following form:
  - When the image file is saved on an FTP server:
    ftp://<IP_address>:<port>/<path>/<image_file_name>.bin
  - When the image file is saved on a TFTP server:
    tftp://<IP_address>/<path>/<image_file_name>.bin
  - When the image file is saved on a SCP or SFTP server:
    scp:// or sftp://<IP_address>/<path>/<image_file_name>.bin
    When you enter the URL without the user name and password, the device displays the Credentials window. There you enter the login credentials needed to log in to the server.
- To start the update procedure, click the Start button.
  The device copies the currently running device software into the backup memory.
  As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
  During the next system startup, the device loads the installed device software.

  enable
  copy firmware remote tftp://10.0.1.159/product.bin system

  To change to the Privileged EXEC mode.

  To transfer the product.bin file from the TFTP server with the IP address 10.0.1.159 to the device.
6.4 Software update from the external memory

6.4.1 Manually—initiated by the administrator

The device lets you update the device software with a few mouse clicks. The prerequisite is that the image file of the device software is located in the external memory.

Perform the following steps:

- Open the Basic Settings > Software dialog.
- Mark the table row which displays the name of the desired image file in the external memory.
- Right-click to display the context menu.
- To start the update procedure, click in the context menu the Update item.
  
  The device copies the currently running device software into the backup memory. As soon as the update procedure is completed successfully, the device displays an information that the software is successfully updated.
  
  During the next system startup, the device loads the installed device software.

6.4.2 Automatically—initiated by the device

When the following files are located in the external memory during the system startup, the device updates the device software automatically:

- the image file of the device software
- a text file startup.txt with the content autoUpdate=<Image_file_name>.bin

The prerequisite is that in the Basic Settings > External Memory dialog, you mark the checkbox in the Software auto update column. This is the default setting in the device.

Perform the following steps:

- Copy the image file of the new device software into the main directory of the external memory. Use only an image file suitable for the device.
- Create a text file startup.txt in the main directory of the external memory.
- Open the startup.txt file in the text editor and add the following line:
  
  autoUpdate=<Image_file_name>.bin

- Install the external memory in the device.
Restart the device.
During the booting process, the device checks automatically the following criteria:
- Is an external memory connected?
- Is a startup.txt file in the main directory of the external memory?
- Does the image file exist which is specified in the startup.txt file?
- Is the software version of the image file more recent than the software currently running in the device?

When the criteria are fulfilled, the device starts the update procedure.
The device copies the currently running device software into the backup memory.
As soon as the update procedure is completed successfully, the device reboots automatically and loads the new software version.

Check the result of the update procedure. The log file in the Diagnostics > Report > System Log dialog contains one of the following messages:
- S_watson AUTOMATIC_SWUPDATE_SUCCESS
  Software update completed successfully
- S_watson AUTOMATIC_SWUPDATE_ABORTED
  Software update aborted
- S_watson AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE
  Software update aborted due to wrong image file
- S_watson AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE
  Software update aborted because the device did not save the image file.
Loading software updates
6.4 Software update from the external memory
7 Configuring the ports

The following port configuration functions are available.

- Enabling/disabling the port
- Selecting the operating mode

7.1 Enabling/disabling the port

In the default setting, every port is enabled. For a higher level of access security, disable unconnected ports. To do this, perform the following steps:

- Open the Basic Settings > Port dialog, Configuration tab.
- To enable a port, mark the checkbox in the Port on column.
- To disable a port, unmark the checkbox in the Port on column.
- Save the settings temporarily. To do this, click the ✓ button.

enable
configure
interface 1/1
no shutdown

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/1.
To enable the interface.
7.2 Selecting the operating mode

In the default setting, the ports are set to Automatic configuration operating mode.

**Note:** The active automatic configuration has priority over the manual configuration.

Perform the following steps:

- Open the **Basic Settings > Port** dialog, **Configuration** tab.
- If the device connected to this port requires a fixed setting, then perform the following steps:
  - Deactivate the function. Unmark the checkbox in the **Automatic configuration** column.
  - In the **Manual configuration** column, specify the desired operating mode (transmission rate, duplex mode).
- Save the settings temporarily. To do this, click the ** ✓ ** button.

```
enable
configure
interface 1/1
no auto-negotiate
speed 100 full
```

- To change to the Privileged EXEC mode.
- To change to the Configuration mode.
- To change to the interface configuration mode of interface 1/1.
- To disable the automatic configuration mode.
- To set port speed 100 MBit/s and full duplex.
8 Assistance in the protection from unauthorized access

The device offers functions that help you protect the device against unauthorized access.

After you set up the device, carry out the following steps in order to reduce possible unauthorized access to the device.

- Changing the SNMPv1/v2 community
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling Telnet
- Disabling HiDiscovery
- Enable IP access restriction
- Adjusting the session timeouts
- Deactivating the unused modules

8.1 Changing the SNMPv1/v2 community

SNMPv1/v2 works unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext community name with which the sender accesses the device. If SNMPv1/v2 is enabled, then the device lets anyone who knows the community name access the device.

The community names public for read accesses and private for write accesses are preset. If you are using SNMPv1 or SNMPv2, then change the default community name. Treat the community names with discretion. To do this, perform the following steps:

   The dialog displays the communities that are set up.
2. For the Write community, specify in the Name column the community name.
   - Up to 32 alphanumeric characters are allowed.
   - The device differentiates between upper and lower case.
   - Specify a different community name than for read access.
3. Save the settings temporarily. To do this, click the ✓ button.

   ```
   enable
   configure
   snmp community rw <community name>
   show snmp community
   save
   ```

   To change to the Privileged EXEC mode.
   To change to the Configuration mode.
   To specify the community for read/write access.
   To display the communities that have been configured.
   To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
8.2 Disabling SNMPv1/v2

If you need SNMPv1 or SNMPv2, then use these protocols only in environments protected from eavesdropping. SNMPv1 and SNMPv2 do not use encryption. The SNMP packets contain the community in clear text. We recommend using SNMPv3 in the device and disabling the access using SNMPv1 and SNMPv2. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SNMP tab. The dialog displays the settings of the SNMP server.
- To deactivate the SNMPv1 protocol, you unmark the SNMPv1 checkbox.
- To deactivate the SNMPv2 protocol, you unmark the SNMPv2 checkbox.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
no snmp access version v1
no snmp access version v2
show snmp access
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To deactivate the SNMPv1 protocol.
To deactivate the SNMPv2 protocol.
To display the SNMP server settings.
To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.
8.3 Disabling HTTP

The web server provides the Graphical User Interface with the protocol HTTP or HTTPS. HTTPS connections are encrypted, while HTTP connections are unencrypted.

The HTTP protocol is enabled by default. If you disable HTTP, then no unencrypted access to the Graphical User Interface is possible. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, HTTP tab.
- To disable the HTTP protocol, select the Off radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✅ button.

To disable the HTTP protocol:

- enable
- configure
- no http server

To change to the Privileged EXEC mode:

- enable
- configure

To change to the Configuration mode:

- https server

If the HTTP protocol is disabled, then you can reach the Graphical User Interface of the device only by HTTPS. In the address bar of the web browser, enter the string https:// before the IP address of the device.

If the HTTPS protocol is disabled and you also disable HTTP, then the Graphical User Interface is unaccessible. To work with the Graphical User Interface, enable the HTTPS server using the Command Line Interface. To do this, perform the following steps:

To change to the Privileged EXEC mode:

- enable
- configure

To change to the Configuration mode:

- https server

To enable the HTTPS protocol:

- enable
- configure
- https server
8.4 Disabling Telnet

The device lets you remotely access the device management using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled in the device by default. If you disable Telnet, then unencrypted remote access to the Command Line Interface is no longer possible. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, Telnet tab.
- To disable the Telnet server, select the off radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
configure
no telnet server
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To disable the Telnet server.

If the SSH server is disabled and you also disable Telnet, then access to the Command Line Interface is only possible through the serial interface of the device. To work remotely with the Command Line Interface, enable SSH. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- To enable the SSH server, select the on radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
configure
ssh server
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To enable the SSH server.
8.5 Disabling the HiDiscovery access

HiDiscovery lets you assign IP parameters to the device over the network during commissioning. HiDiscovery communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, we recommend to set HiDiscovery to read-only or to disable HiDiscovery access completely. To do this, perform the following steps:

- Open the Basic Settings > Network > Global dialog.
- To take away write permission from the HiDiscovery software, in the HiDiscovery protocol v1/v2 frame, specify the value `readOnly` in the Access field.
- To disable HiDiscovery access completely, select the `Off` radio button in the HiDiscovery protocol v1/v2 frame.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
network hidiscovery mode read-only
no network hidiscovery operation
```

To change to the Privileged EXEC mode.

To disable write permission of the HiDiscovery software.

To disable HiDiscovery access.
8.6 **Activating the IP access restriction**

In the default setting, you access the device management from any IP address and with the supported protocols.

The IP access restriction lets you restrict access to the device management to selected IP address ranges and selected IP-based protocols.

Example:

The device is to be accessible only from the company network using the Graphical User Interface. The administrator has additional remote access using SSH. The company network has the address range 192.168.1.0/24 and remote access from a mobile network with the IP address range 109.237.176.0/24. The SSH application program knows the fingerprint of the RSA key.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Company network</th>
<th>Mobile phone network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network address</td>
<td>192.168.1.0</td>
<td>109.237.176.0</td>
</tr>
<tr>
<td>Netmask</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Desired protocols</td>
<td>https, snmp</td>
<td>ssh</td>
</tr>
</tbody>
</table>

Perform the following steps:

- Open the **Device Security > Management Access > IP Access Restriction** dialog.
- Unmark the checkbox in the **Active** column for the table row.
  - This entry lets users have access to the device from any IP address and the supported protocols.

Address range of the company network:

- To add a table row, click the **button.**
- Specify the address range of the company network in the **IP address range** column: 192.168.1.0/24
- For the address range of the corporate network, deactivate the undesired protocols. The **HTTPS, SNMP**, and **Active** checkboxes remain marked.

Address range of the mobile phone network:

- To add a table row, click the **button.**
- Specify the address range of the mobile network in the **IP address range** column: 109.237.176.0/24
- For the address range of the mobile network, deactivate the undesired protocols. The **SSH** and **Active** checkboxes remain marked.

Before you enable the function, verify that at least one active table row lets you have access. Otherwise, if you change the settings, then the connection to the device terminates. Access to the device management is only possible using the Command Line Interface through the serial interface of the device.

- To enable IP access restriction, select the **On** radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the **✓** button.
enable
show network management access global

show network management access rules
no network management access operation
network management access add 2

network management access modify 2 ip 192.168.1.0
network management access modify 2 mask 24
network management access modify 2 ssh disable

network management access add 3

network management access modify 3 ip 109.237.176.0
network management access modify 3 mask 24
network management access modify 3 snmp disable

no network management access status 1
network management access status 2
network management access status 3
show network management access rules
network management access operation

To change to the Privileged EXEC mode.
To display if IP access restriction is enabled or disabled.
To display the entries that have been configured.
To disable the IP access restriction.
To create the entry for the address range of the company network.
Number of the next available index in this example: 2.
To specify the IP address of the company network.
To specify the netmask of the company network.
To deactivate SSH for the address range of the company network.
Repeat the operation for every unwanted protocol.
To create an entry for the address range of the mobile phone network.
Number of the next available index in this example: 3.
To specify the IP address of the mobile phone network.
To specify the netmask of the mobile phone network.
To deactivate SNMP for the address range of the mobile phone network.
Repeat the operation for every unwanted protocol.
To deactivate the default entry.
This entry lets users have access to the device from any IP address and the supported protocols.
To activate an entry for the address range of the company network.
To activate an entry for the address range of the mobile phone network.
To display the entries that have been configured.
To enable the IP access restriction.
8.7 Adjusting the session timeouts

The device lets you automatically terminate the session upon inactivity of the logged-on user. The session timeout is the period of inactivity after the last user action.

You can specify a session timeout for the following applications:
- Command Line Interface sessions using an SSH connection
- Command Line Interface sessions using a Telnet connection
- Command Line Interface sessions using a serial connection
- Graphical User Interface

**Timeout for Command Line Interface sessions using a SSH connection**

Perform the following steps:

- Open the **Device Security > Management Access > Server** dialog, **SSH** tab.
- Specify the timeout period in minutes in the **Configuration** frame, **Session timeout [min]** field.
- Save the settings temporarily. To do this, click the **✓** button.

```
enable
configure
ssh timeout <0..160>
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the timeout period in minutes for Command Line Interface sessions using an SSH connection.

**Timeout for Command Line Interface sessions using a Telnet connection**

Perform the following steps:

- Open the **Device Security > Management Access > Server** dialog, **Telnet** tab.
- Specify the timeout period in minutes in the **Configuration** frame, **Session timeout [min]** field.
- Save the settings temporarily. To do this, click the **✓** button.

```
enable
configure
telnet timeout <0..160>
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the timeout period in minutes for Command Line Interface sessions using a Telnet connection.
### Timeout for Command Line Interface sessions using a serial connection

Perform the following steps:

- Open the Device Security > Management Access > CLI dialog, Global tab.
- Specify the timeout period in minutes in the Configuration frame, Serial interface timeout [min] field.
- Save the settings temporarily. To do this, click the ✔ button.

```
enable
cli serial-timeout <0..160>
```

To change to the Privileged EXEC mode.
To specify the timeout period in minutes for Command Line Interface sessions using a serial connection.

### Session timeout for the Graphical User Interface

Perform the following steps:

- Open the Device Security > Management Access > Web dialog.
- Specify the timeout period in minutes in the Configuration frame, Web interface session timeout [min] field.
- Save the settings temporarily. To do this, click the ✔ button.

```
enable
network management access web timeout <0..160>
```

To change to the Privileged EXEC mode.
To specify the timeout period in minutes for Graphical User Interface sessions.
8.8 **Deactivating the unused modules**

The default settings of a media module slot allow access to the network. If a media module is inserted into an empty slot, the media module ports will establish network connections by default.

To help prevent unauthorized network access, deactivate the unused slots. To do this, perform the following steps:

- Open the *Basic Settings > Modules* dialog.
- To deactivate the slot and deny network access, unmark the *Active* checkbox.
- Save the settings temporarily. To do this, click the ✅ button.
9 **Controlling the data traffic**

The device checks the data packets to be forwarded in accordance with defined rules. Data packets to which the rules apply are either forwarded by the device or blocked. If data packets do not correspond to any of the rules, then the device blocks the packets.

Routing ports to which no rules are assigned allow packets to pass. As soon as a rule is assigned, the assigned rules are processed first. After that, the specified standard action of the device takes effect.

The device provides the following functions for controlling the data stream:

- Service request control (Denial of Service, DoS)
- Denying access to devices based on their IP or MAC address (ACL)

The device observes and monitors the data stream. The device takes the results of the observation and the monitoring and combines them with the rules for the network security to create what is known as a status table. Based on this status table, the device decides whether to accept, drop or reject data.

The data packets go through the filter functions of the device in the following sequence:

- DoS ... if permit or accept, then progress to the next rule
- ACL ... if permit or accept, then progress to the next rule

9.1 **Helping protect against DoS attacks**

DoS is a cyber-attack that aims to bring down specific services or devices. Attackers as well as network administrators can use the port scan method to discover open ports in a network to find vulnerable devices. The function helps you protect your network against invalid or falsified data packets targeted at certain services or devices. You have the option of specifying filters in order to restrict the data stream for protection against DoS attacks. The filters check the received data packets. The device discards a data packet if it matches the filter criteria.

To help protect the device itself and other devices in the network from DoS attacks, the device lets you specify the following filters:

- Filters for TCP and UDP packets
- Filters for IP packets
- Filters for ICMP packets

The filters help prevent an attacking station from:

- Detecting services and applications that use the open ports
- Detecting active devices in a network
- Accessing sensitive data in a network
- Detecting active security devices like a firewall used in a network

**Note:** You can combine the filters in any way. When you activate several filters, the device applies the filters in the order in which they are specified in the IP table. If an incoming data packet matches a filter, the device discards the respective data packet and then stops further processing.
9.1.1 Filters for TCP and UDP packets

To selectively process TCP and UDP packets, the device offers you the following filters:

- Activate the Null Scan filter function
- Activate the Xmas filter function
- Activate the SYN/FIN filter function
- Activate the TCP Offset protection function
- Activate the TCP SYN protection function
- Activate the L4 Port protection function
- Activate the Min. Header Size filter function

Activate the Null Scan filter function

With the Null Scan method, the attacking station sends data packets with the following properties:

- No TCP flags are set.
- The TCP sequence number is 0.

The device uses the Null Scan filter function to discard incoming TCP packets that contain malicious properties.

In the default setting, the Null Scan filter function is disabled. To activate the Null Scan filter function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the Null Scan filter function. To do this, in the TCP/UDP frame, mark the Null Scan filter checkbox.
- Save the settings temporarily. To do this, click the button.

activate
cfg

dos tcp-null

no dos tcp-null

activate

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To activate the Null Scan filter function.

To deactivate the Null Scan filter function.

Activate the Xmas filter function

With the Xmas method, the attacking station sends data packets with the following properties:

- The TCP flags FIN, URG, and PSH are simultaneously set.
- The TCP sequence number is 0.

The device uses the Xmas filter function to discard incoming TCP packets that contain malicious properties.
In the default setting, the Xmas filter function is disabled. To activate the Xmas filter function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the Xmas filter function. To do this, in the TCP/UDP frame, mark the Xmas filter checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

**Activate the SYN/FIN filter function**

With the SYN/FIN method, the attacking station sends data packets with the TCP flags SYN and FIN set simultaneously. The device uses the SYN/FIN filter function to discard incoming packets with the TCP flags SYN and FIN set simultaneously.

In the default setting, the SYN/FIN filter function is disabled. To activate the SYN/FIN filter function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the SYN/FIN filter function. To do this, in the TCP/UDP frame, mark the SYN/FIN filter checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

**Activate the TCP Offset protection function**

With the TCP Offset method, the attacking station sends data packets whose fragment offset is equal to 1. The fragment offset is a field in the IP header which helps to identify the sequence of fragments in received data packets. The device uses the TCP Offset protection function to discard incoming TCP data packets whose fragment offset field in the IP header is equal to 1.

**Note:** The device accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1.
In the default setting, the TCP Offset protection function is disabled. To activate the TCP Offset protection function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the TCP Offset protection function. To do this, in the TCP/UDP frame, mark the TCP Offset protection checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

TCP Offset protection

Activate the TCP SYN protection function

With the TCP SYN method, the attacking station sends data packets with the TCP flag SYN set and an L4 (layer 4) source port <1024. The device uses the TCP SYN protection function to discard incoming packets with the TCP flag SYN set and an L4 source port <1024.

In the default setting, the TCP SYN protection function is disabled. To activate the TCP SYN protection function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the TCP SYN protection function. To do this, in the TCP/UDP frame, mark the TCP SYN protection checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

TCP SYN protection

enable
configure
dos tcp-offset
no dos tcp-offset

to change to the Privileged EXEC mode.
to change to the Configuration mode.
to activate the TCP Offset protection function.
to deactivate the TCP Offset protection function.

to change to the Privileged EXEC mode.
to change to the Configuration mode.
to activate the TCP SYN protection function.
to deactivate the TCP SYN protection function.
Controlling the data traffic

9.1 Helping protect against DoS attacks

Activate the L4 Port protection function

An attacking station can send TCP or UDP data packets whose source port number and destination port number are identical. The device uses the L4 Port protection function to discard incoming TCP and UDP packets whose L4 source port and destination port number are identical.

In the default setting, the L4 Port protection function is disabled. To activate the L4 Port protection function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the L4 Port protection function. To do this, in the TCP/UDP frame, mark the L4 Port protection checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

`enable`
To change to the Privileged EXEC mode.
`configure`
To change to the Configuration mode.
`dos 14-port`
To activate the L4 Port protection function.
`no dos 14-port`
To deactivate the L4 Port protection function.

Activate the Min. Header Size filter function

The device uses the Min. Header Size filter function to check the TCP header of received data packets. The device discards the data packet when (data offset value × 4) < minimum TCP header size.

The Min. Header Size filter function detects received data packets with the following properties:

(IP payload length in the IP header - IP header outer size) < minimum TCP header size.

In the default setting, the Min. Header Size filter function is disabled. To activate the Min. Header Size filter function, perform the following steps:

- Open the Network Security > DoS > Global dialog.
- Activate the Min. Header Size filter function. To do this, in the TCP/UDP frame, mark the Min. Header Size filter checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

`enable`
To change to the Privileged EXEC mode.
`configure`
To change to the Configuration mode.
`dos tcp-min-header`
To activate the Min. Header Size filter function.
`no dos tcp-min-header`
To deactivate the Min. Header Size filter function.
9.1.2 Filters for IP packets

To selectively process IP packets, the device offers you the following filters:

- Activate the Land Attack filter function

Activate the Land Attack filter function

With the Land Attack method, the attacking station sends data packets whose source and destination addresses are identical to the IP address of the recipient. The device uses the Land Attack filter function to discard received packets whose source and destination addresses are identical.

In the default setting, the Land Attack filter function is disabled. To activate the Land Attack filter function, perform the following steps:

2. Activate the Land Attack filter function. To do this, in the IP frame, mark the Land Attack filter checkbox.
3. Save the settings temporarily. To do this, click the ✓ button.

```
enable
configure
dos ip-land enable
no dos ip-land disable
```

9.1.3 Filters for ICMP packets

To selectively process ICMP packets, the device offers you the following filters:

- Activate the Fragmented packets filter function
- Activate the Packet size filter function

Activate the Fragmented packets filter function

The device uses the Fragmented packets filter function to protect the network from attacking stations that send fragmented ICMP packets. Fragmented ICMP packets can cause the destination device to fail if the destination device processes fragmented ICMP packets incorrectly. The device uses the Fragmented packets filter function to discard fragmented ICMP packets.

In the default setting, the Fragmented packets filter function is disabled. To activate the Fragmented packets filter function, perform the following steps:

2. Activate the Fragmented packets filter function. To do this, in the ICMP frame, mark the Fragmented packets filter checkbox.
3. Save the settings temporarily. To do this, click the ✓ button.
Helping protect against DoS attacks

9.1 Controlling the data traffic

Activate the Packet size filter function

The device uses the **Packet size filter** to discard data packets whose payload size exceeds the size specified in the **Allowed payload size [byte]** field.

The **Packet size filter** function helps protect the network from attacking stations that send **ICMP** packets whose payload size exceeds the size specified in the **Allowed payload size [byte]** field.

In the default setting, the **Packet size filter** function is disabled. To activate the **Packet size filter** function, perform the following steps:

1. Open the **Network Security > DoS > Global** dialog.
2. Activate the **Packet size filter** function. To do this, in the **ICMP** frame, mark the **Packet size filter** checkbox.
3. Save the settings temporarily. To do this, click the **✓** button.

---

<table>
<thead>
<tr>
<th>enable</th>
<th>configure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dos icmp-fragmented</td>
</tr>
<tr>
<td></td>
<td>no dos icmp-fragmented</td>
</tr>
</tbody>
</table>

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To activate the **Fragmented packets filter** function.
To deactivate the **Fragmented packets filter** function.

---

<table>
<thead>
<tr>
<th>enable</th>
<th>configure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dos icmp payload-check</td>
</tr>
<tr>
<td></td>
<td>no dos icmp payload-check</td>
</tr>
</tbody>
</table>

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To activate the **Packet size filter** function.
To deactivate the **Packet size filter** function.
In this menu you can enter the parameters for the Access Control Lists (ACLs).

The device uses ACLs to filter data packets received on VLANs or on individual or multiple ports. In a ACL, you specify rules that the device uses to filter data packets. When such a rule applies to a packet, the device applies the actions specified in the rule to the packet. The available actions are as follows:

- allow (permit)
- discard (deny)
- redirect to a certain port (see *Redirection port* field)
- mirror (see *Mirror port* field)

The list below contains criteria that you can apply to filter the data packets:

- Source or destination address of a packet (MAC)
- Source or destination address of a data packet (IPv4)
- Source or destination port of a data packet (IPv4)

You can specify the following ACL types:

- IP ACLs for VLANs
- IP ACLs for ports
- MAC ACLs for VLANs
- MAC ACLs for ports

When you assign both an IP ACL and MAC ACL to the same interface, the device first uses the IP ACL to filter the data stream. The device applies the MAC ACL rules only after the packets are filtered through the IP ACL. The priority of an ACL is independent of the index of a rule.

Within an ACL, the device processes the rules in order. The index of the respective rule determines the order in which the device filters the data stream. When you assign an ACL to a port or VLAN, you can specify its priority with the index. The lower the number, the higher the priority. The device processes the rule with the higher priority first.

If none of the rules specified in an ACL applies to a data packet, then the implicit *deny* rule applies. As a result, the device drops the received data packets.

Keep in mind that the device directly implements the implicit *deny* rule.

**Note:** The number of available ACLs depends on the device. For further information about the ACL values, see chapter "Technical Data" on page 320.

**Note:** You can assign a single ACL to any number of ports or VLANs.

The ACL menu contains the following dialogs:

- *IPv4 Rule*
- *MAC Rule*
- *Assignment*

These dialogs provide the following options:

- To specify the rules for the various ACL types.
- To provide the rules with the required priorities.
- To assign the ACLs to ports or VLANs.
9.2.1 Creating and editing IPv4 rules

When filtering IPv4 data packets, the device lets you:

- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules

Perform the following steps:

2. Click the + button.
   The dialog displays the Create window.
3. Specify the name of the ACL (group).
   - To create the rule in an existing ACL, click the Group name field and select the name from the drop-down list.
   - To create the rule in a new ACL, specify a meaningful name in the Group name field and click the + icon.
4. In the Index field you specify the number for the rule within the ACL.
   This number defines the priority of the rule.
5. Click the Ok button.
   The device adds the rule to the ACL (group) in the table.
   The rule is active immediately.
6. To remove a rule, select the desired table row and click the - button.
7. Edit the rule parameters in the table. To change a value, double-click the relevant field.
8. Save the settings temporarily. To do this, click the ✓ button.

Note: The device lets you use wildcards with the Source IP address and Destination IP address parameters. If you enter for example, 192.168.?.?, then the device allows addresses that start with 192.168.

Note: The prerequisite for changing the values in the Source TCP/UDP port and Destination TCP/UDP port column is that you specify the value tcp or udp in the Protocol column.

Note: The prerequisite for changing the value in the Redirection port and Mirror port column is that you specify the value permit in the Action column.
9.2.2 Creating and configuring an IP ACL using the Command Line Interface

In the following example, you configure ACLs to block communications from computers B and C, to computer A based on the IP (TCP, UDP, etc.).

Perform the following steps:

```
enable  
configure  
```

To change to the Privileged EXEC mode.

```
configure  
```

To change to the Configuration mode.

To add an IP ACL with name `filter1`. To add a rule denying IP data packets from 10.0.1.11 to 10.0.1.158. Priority 1 (highest priority).

```
ip access-list extended name filter1
deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1
```

To add a rule to the IP ACL admitting IP data packets.

```
ip access-list extended name filter1
permit src any dst any
```

To display the rules of the IP ACL `filter1`.

```
show access-list ip filter1
```

To add an IP ACL with name `filter2`. To add a rule denying IP data packets from 10.0.1.13 to 10.0.1.158. Priority 1 (highest priority).

```
ip access-list extended name filter2
deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1
```

To display the rules of the IP ACL `filter2`.

```
show access-list ip filter2
```

9.2.3 Creating and editing MAC rules

When filtering MAC data packets, the device lets you:

- create new groups and rules
- add new rules to existing groups
- edit an existing rule
- activate and deactivate groups and rules
- delete existing groups and rules
- change the order of existing rules
Perform the following steps:

- Open the **Network Security > ACL > MAC Rule** dialog.
- Click the **button.**
  The dialog displays the **Create** window.
- Specify the name of the ACL (group).
  - To create the rule in an existing ACL, click the **Group name** field and select the name from the drop-down list.
  - To create the rule in a new ACL, specify a meaningful name in the **Group name** field and click the **icon.**
- In the **Index** field you specify the number for the rule within the ACL. This number defines the priority of the rule.
- Click the **Ok** button.
  The device adds the rule to the ACL (group) in the table.
  The rule is active immediately.
- To remove a rule, select the desired table row and click the **button.
- Edit the rule parameters in the table. To change a value, double-click the relevant field.
- Save the settings temporarily. To do this, click the **button.

**Note:** In the **Source MAC address** and **Destination MAC address** fields you can use wildcards in the **FF:??::??::??::??** or **??::??::??::00:01** form. Use capital letters here.

### 9.2.4 Creating and configuring a MAC ACL using the Command Line Interface

In the following example, AppleTalk and IPX are to be filtered out from the entire network. To do this, perform the following steps:

```plaintext
enable
cfg
mac acl add 1 macfilter

mac acl rule add 1 1 deny src any any dst any any etype appletalk

mac acl rule add 1 2 deny src any any dst any any etype ipx-old

mac acl rule add 1 3 deny src any any dst any any etype ipx-new

mac acl rule add 1 4 permit src any any dst any any

show acl rules 1

interface 1/1,1/2,1/3,1/4,1/5,1/6
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To add an MAC ACL with the ID 1 and the name **macfilter**.
To add a rule to position 1 of the MAC ACL with the ID 1 rejecting packets with EtherType **0x809B (AppleTalk)**.
To add a rule to position 2 of the MAC ACL with the ID 1 rejecting packets with EtherType **0x8137 (IPX alt)**.
To add a rule to position 3 of the MAC ACL with the ID 1 rejecting packets with EtherType **0x8138 (IPX)**.
To add a rule to position 4 of the MAC ACL with the ID 1 forwarding packets.
To display the rules of the MAC ACL with the ID 1.
To change to the interface configuration mode of the interfaces 1/1 to 1/6.
9.2.5 Assigning ACLs to a port or VLAN

When you assign ACLs to a port or VLAN, the device gives you the following options:
- To select the port or VLAN.
- To specify the ACL priority.
- To select the ACL using the group name.

Perform the following steps:

- Open the Network Security > ACL > Assignment dialog.
- Click the  button. The dialog displays the Create window.
- In the Port/VLAN field, specify the desired port or the desired VLAN.
- In the Priority field, specify the priority.
- In the Direction field, specify the data packets to which the device applies the rule.
- In the Group name field, specify the rule the device assigns to the port or the VLAN.
- Click the Ok button.
- Save the settings temporarily. To do this, click the ✓ button.
10 Network load control

The device features a number of functions that can help you reduce the network load:

- Direct packet distribution
- Multicasts
- Rate limiter
- Prioritization - QoS
- Flow control

10.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination “port and MAC address” in its MAC address table (FDB).

By applying the “Store and Forward” method, the device buffers data received and checks it for validity before forwarding it. The device rejects invalid and defective data packets.

10.1.1 Learning MAC addresses

When the device receives a data packet, it checks if the MAC address of the sender is already stored in the MAC address table (FDB). When the MAC address of the sender is unknown, the device generates a new entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (FDB):

- The device forwards packets with a known destination MAC address directly to ports that have already received data packets from this MAC address.
- The device floods data packets with unknown destination addresses, that is, the device forwards these data packets to every port.

10.1.2 Aging of learned MAC addresses

Addresses that have not been detected by the device for an adjustable period of time (aging time) are deleted from the MAC address table (FDB) by the device. A reboot or resetting of the MAC address table deletes the entries in the MAC address table (FDB).

10.1.3 Static address entries

In addition to learning the sender MAC address, the device also provides the option to set MAC addresses manually. These MAC addresses remain configured and survive resetting of the MAC address table (FDB) as well as rebooting of the device.

Static address entries allow the device to forward data packets directly to selected ports. If you do not specify a destination port, then the device discards the corresponding data packets.
You manage the static address entries in the Graphical User Interface or in the Command Line Interface.

Perform the following steps:
☐ Create a static address entry.

☐ Open the Switching > Filter for MAC Addresses dialog.
☐ Add a user-configurable MAC address:
  ▶  Click the button.
  The dialog displays the Create window.
  ▶  In the Address field, specify the destination MAC address.
  ▶  In the VLAN ID field, specify the ID of the VLAN.
  ▶  In the Port list, select the ports to which the device forwards data packets with the specified destination MAC address in the specified VLAN.
  When you have defined a Unicast MAC address in the Address field, select only one port.
  When you have defined a Multicast MAC address in the Address field, select one or more ports.
  If you want the device to discard data packets with the destination MAC address, then do not select any port.
  ▶  Click the Ok button.

☐ Save the settings temporarily. To do this, click the button.
Network load control

10.1 Direct packet distribution

- Convert a learned MAC address into a static address entry.
  - Open the **Switching > Filter for MAC Addresses** dialog.
  - To convert a learned MAC address into a static address entry, select the value **permanent** in the **Status** column.
  - Save the settings temporarily. To do this, click the **✓** button.

- Disable a static address entry.
  - Open the **Switching > Filter for MAC Addresses** dialog.
  - To disable a static address entry, remove it from the table. To do this, select the table row that contains the value **permanent** in the **Status** column, then click the **✘** button.
  - Save the settings temporarily. To do this, click the **✓** button.

- Delete learned MAC addresses.
  - To delete the learned addresses from the MAC address table (FDB), click the **🗑** button. Alternatively, open the **Basic Settings > Restart** dialog and click the **Reset MAC address table** button.
clear mac-addr-table

To delete the learned MAC addresses from the MAC address table (FDB).
10.2 Multicasts

By default, the device floods data packets with a Multicast address, that is, the device forwards the data packets to every port. This leads to an increased network load.

The use of IGMP snooping can reduce the network load caused by Multicast data traffic. IGMP snooping lets the device send Multicast data packets only on those ports to which devices “interested” in Multicast are connected.

10.2.1 Example of a Multicast application

Surveillance cameras transmit images to monitors in the machine room and in the monitoring room. With an IP Multicast transmission, the cameras transmit their graphic data over the network in Multicast packets.

The Internet Group Management Protocol (IGMP) organizes the Multicast data traffic between the Multicast routers and the monitors. The switches in the network between the Multicast routers and the monitors monitor the IGMP data traffic continuously (“IGMP Snooping”).

Switches register logins for receiving a Multicast stream (IGMP report). The device then creates an entry in the MAC address table (FDB) and forwards Multicast packets only to the ports on which it has previously received IGMP reports.

10.2.2 IGMP snooping

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and connected receivers on Layer 3. IGMP Snooping describes the function of a switch of continuously monitoring IGMP traffic and optimizing its own transmission settings for this data traffic.

The IGMP Snooping function in the device operates according to RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast routers with an active IGMP function periodically request (query) registration of Multicast streams in order to determine the associated IP Multicast group members. IP Multicast group members reply with a Report message. This Report message contains the parameters required by the IGMP function. The Multicast router enters the IP Multicast group address from the Report message in its routing table. This causes it to forward data packets with this IP Multicast group in the destination address field according to its routing table.

When leaving a Multicast group (IGMP version 2 and higher), receivers log out with a “Leave” message and do not send any more Report messages. If it does not receive any more Report messages from this receiver within a certain time (aging time), then the Multicast router removes the routing table entry of a receiver.

When several IGMP Multicast routers are in the same network, the device with the smaller IP address takes over the query function. When there are no Multicast routers on the network, you have the option to enable the query function in an appropriately equipped switch.

A switch that connects one Multicast receiver with a Multicast router analyzes the IGMP information with the IGMP snooping method.
The IGMP snooping method also makes it possible for switches to use the IGMP function. A switch stores the MAC addresses derived from IP addresses of the Multicast receivers as recognized Multicast addresses in its MAC address table (FDB). In addition, the switch identifies the ports on which it has received reports for a specific Multicast address. In this way, the switch forwards Multicast packets only to ports to which Multicast receivers are connected. The other ports do not receive these packets.

A special feature of the device is the possibility of determining the processing of data packets with unknown Multicast addresses. Depending on the setting, the device discards these data packets or forwards them to every port. By default, the device transmits the data packets only to ports with connected devices, which in turn receive query packets. You also have the option of additionally sending known Multicast packets to query ports.

**Setting IGMP snooping**

Perform the following steps:

- Open the Switching > IGMP Snooping > Global dialog. To enable the function, select the On radio button in the Operation frame.
- When the IGMP Snooping function is disabled, the device behaves as follows:
  - The device ignores the received query and report messages.
  - The device forwards (floods) received data packets with a Multicast address as the destination address to every port.
- Save the settings temporarily. To do this, click the ✓ button.

- Specifying the settings for a port:
  - Open the Switching > IGMP Snooping > Configuration dialog, Port tab.
  - To activate the IGMP Snooping function on a port, mark the checkbox in the Active column for the relevant port.
  - Save the settings temporarily. To do this, click the ✓ button.

- Specifying the settings for a VLAN:
  - Open the Switching > IGMP Snooping > Configuration dialog, VLAN ID tab.
  - To activate the IGMP Snooping function for a specific VLAN, mark the checkbox in the Active column for the relevant VLAN.
  - Save the settings temporarily. To do this, click the ✓ button.

**Setting the IGMP querier function**

The device itself optionally sends active query messages; alternatively, it responds to query messages or detects other Multicast queriers in the network (Querier function).

Prerequisite:
The **IGMP Snooping** function is enabled globally.

Perform the following steps:

- Open the **Switching > IGMP Snooping > Querier** dialog.
- In the **Operation** frame, enable/disable the **Querier** function of the device globally.
- To activate the **Querier** function for a specific VLAN, mark the checkbox in the **Active** column for the relevant VLAN.
  - The device carries out a simple selection process: When the IP source address of the other Multicast querier is lower than its own, the device switches to the passive state, in which it does not send out any more query requests.
  - In the **Address** column, you specify the IP Multicast address that the device inserts as the sender address in generated query requests. You use the address of the Multicast router.
- Save the settings temporarily. To do this, click the ✔ button.

### IGMP snooping enhancements (table)

The **Switching > IGMP Snooping > Snooping Enhancements** dialog provides you access to enhanced settings for the **IGMP Snooping** function. You activate or deactivate the settings on a per port basis in a VLAN.

The following settings are possible:

- **Static**
  - Use this setting to set the port as a static query port. The device forwards every IGMP message on a static query port, even if it has previously received no IGMP query messages on this port. When the static option is disabled and the device has previously received IGMP query messages, it forwards IGMP messages on this port. When this is the case, the entry displays L (“learned”).
  - Learn by LLDP
    - A port with this setting automatically discovers other Hirschmann devices using LLDP (Link Layer Discovery Protocol). The device then learns the IGMP query status of this port from these Hirschmann devices and configures the **Querier** function accordingly. The **ALA** entry indicates that the **Learn by LLDP** function is active. When the device has found another Hirschmann device on this port in this VLAN, the entry also displays an A (“automatic”).
  - Forward All
    - With this setting, the device forwards the data packets addressed to a Multicast address to this port. The setting is suitable in the following situations, for example:
      - For diagnostic purposes.
      - For devices in an MRP Ring: After the ring is switched, the **Forward All** function makes it possible to reconfigure the network rapidly for data packets with registered Multicast destination addresses. Activate the **Forward All** function on every ring port.

**Prerequisite:**

The **IGMP Snooping** function is enabled globally.

Perform the following steps:

- Open the **Switching > IGMP Snooping > Snooping Enhancements** dialog.
- Double-click the desired port in the desired VLAN.
Configure Multicasts

The device lets you configure the exchange of Multicast data packets. The device provides different options depending on whether the data packets are to be sent to unknown or known Multicast receivers.

The settings for unknown Multicast addresses are global for the entire device. The following options can be selected:

- The device discards unknown Multicasts.
- The device forwards unknown Multicasts to every port.
- The device forwards unknown Multicasts only to ports that have previously received query messages (query ports).

Note: The exchange settings for unknown Multicast addresses also apply to the reserved IP addresses from the “Local Network Control Block” (224.0.0.0..224.0.0.255). This behavior can affect higher-level routing protocols.

IGMP Snooping explicitly ignores the following Multicast IP addresses because their mapped Multicast MAC addresses have special functions:

Table 20: Multicast IP addresses ignored by IGMP Snooping

<table>
<thead>
<tr>
<th>Multicast IP Address(es)</th>
<th>Multicast MAC Address(es)</th>
<th>Protocols (Block)</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0..224.0.0.255</td>
<td>01:00:5e:00:00:00..01:00:5e:00:ff</td>
<td>Local Network Control Block</td>
</tr>
<tr>
<td>224.0.1.1</td>
<td>01:00:5e:00:01:01</td>
<td>NTP/SNTP (Internetwork Control Block)</td>
</tr>
<tr>
<td>224.0.1.129..224.0.1.132</td>
<td>01:00:5e:00:18:81..01:00:5e:00:84</td>
<td>PTP (Internetwork Control Block)</td>
</tr>
<tr>
<td>239.255.16.12</td>
<td>01:00:5e:7f:10:0c</td>
<td>HiDiscovery v2 (Administratively Scoped Block)</td>
</tr>
</tbody>
</table>

Note: According to RFC1112 (Host Extensions for IP Multicasting), up to 32 Multicast IP addresses are mapped to the same Multicast MAC address. The table contains only the commonly used Multicast IP address for a Multicast MAC address, omitting the 31 further possible Multicast IP addresses.
For each VLAN, you specify the sending of Multicast packets to known Multicast addresses individually. The following options can be selected:

- The device forwards known Multicasts to the ports that have previously received query messages (query ports) and to the registered ports. Registered ports are ports with Multicast receivers registered with the corresponding Multicast group. This option helps ensure that the transfer works with basic applications without further configuration.
- The device forwards known Multicasts only to the registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution.

Prerequisite:

The *IGMP Snooping* function is enabled globally.

Perform the following steps:

- Open the *Switching > IGMP Snooping > Multicasts* dialog.
- In the *Configuration* frame, you specify how the device forwards data packets to unknown Multicast addresses.
- In the table, you specify how the device forwards data packets to known Multicast addresses.
  - *send to query and registered ports*
    - The device forwards data packets with a known MAC/IP Multicast address to the query ports and to the registered ports.
  - *send to registered ports*
    - The device forwards data packets with a known MAC/IP Multicast address to registered ports.
- Save the settings temporarily. To do this, click the ✔ button.
10.3 Rate limiter

The rate limiter function helps ensure stable operation even with high traffic volumes by limiting traffic on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound traffic.

If the data rate on a port exceeds the defined limit, then the device discards the overload on this port.

Rate limitation occurs entirely on Layer 2. In the process, the rate limiter function ignores protocol information on higher levels such as IP or TCP. This can affect the TCP traffic.

To minimize these effects, use the following options:
- Limit the rate limitation to certain packet types, for example, Broadcasts, Multicasts, and Unicasts with an unknown destination address.
- Limit the outbound data traffic instead of the inbound traffic. The outbound rate limitation works better with TCP flow control due to device-internal buffering of the data packets.
- Increase the aging time for learned Unicast addresses.

Perform the following steps:

- Open the Switching > Rate Limiter dialog.
  - Activate the rate limiter and set limits for the data rate. The settings apply on a per port basis and are broken down by type of traffic:
    - Received Broadcast data packets
    - Received Multicast data packets
    - Received Unicast data packets with an unknown destination address
  
  To activate the rate limiter on a port, mark the checkbox for at least one category. In the Threshold unit column, you specify if the device interprets the threshold values as percent of the port bandwidth or as packets per second. The threshold value 0 deactivates the rate limiter.

- Save the settings temporarily. To do this, click the ✔️ button.
10.4 QoS/Priority

QoS (Quality of Service) is a procedure defined in IEEE 802.1D which is used to distribute resources in the network. QoS lets you prioritize the data of necessary applications.

When there is a heavy network load, prioritizing helps prevent data traffic with lower priority from interfering with delay-sensitive data traffic. Delay-sensitive data traffic includes, for example, voice, video, and real-time data.

10.4.1 Description of prioritization

For data traffic prioritization, traffic classes are defined in the device. The device prioritizes higher traffic classes over lower traffic classes. The number of traffic classes depends on the device type.

To provide for optimal data flow for delay-sensitive data, you assign higher traffic classes to this data. You assign lower traffic classes to data that is less sensitive to delay.

Assigning traffic classes to the data

The device automatically assigns traffic classes to inbound data (traffic classification). The device takes the following classification criteria into account:

- Methods according to which the device carries out assignment of received data packets to traffic classes:
  - trustDot1p
    - The device uses the priority of the data packet contained in the VLAN tag.
  - trustIpDscp
    - The device uses the QoS information contained in the IP header (ToS/DiffServ).
  - untrusted
    - The device ignores possible priority information within the data packets and uses the priority of the receiving port directly.
  - The priority assigned to the receiving port.

Both classification criteria are configurable.

During traffic classification, the device uses the following rules:

- When the receiving port is set to trustDot1p (default setting), the device uses the data packet priority contained in the VLAN tag. When the data packets do not contain a VLAN tag, the device is guided by the priority of the receiving port.
- When the receiving port is set to trustIpDscp, the device uses the QoS information (ToS/DiffServ) in the IP header. When the data packets do not contain IP packets, the device is guided by the priority of the receiving port.
- When the receiving port is set to untrusted, the device is guided by the priority of the receiving port.
Prioritizing traffic classes

For prioritization of traffic classes, the device uses the following methods:

- **Strict Priority**
  When transmission of data of a higher traffic class is no longer taking place or the relevant data is still in the queue, the device sends data of the corresponding traffic class. If every traffic class is prioritized according to the Strict Priority method, then under high network load the device can permanently block the data of lower traffic classes.

- **Weighted Fair Queuing**
  The traffic class is assigned a specific bandwidth. This helps ensure that the device sends the data traffic of this traffic class, although there is a great deal of data traffic in higher traffic classes.

10.4.2 Handling of received priority information

Applications label data packets with the following prioritization information:

- VLAN priority based on IEEE 802.1Q/802.1D (Layer 2)
- Type-of-Service (ToS) or DiffServ (DSCP) for VLAN Management IP packets (Layer 3)

The device lets you evaluate this priority information using the following options:

- **trustDot1p**
  The device assigns VLAN-tagged data packets to the different traffic classes according to their VLAN priorities. The corresponding allocation is configurable. The device assigns the priority of the receiving port to data packets it receives without a VLAN tag.

- **trustIpDscp**
  The device assigns the IP packets to the different traffic classes according to the DSCP value in the IP header, although the packet was also VLAN-tagged. The corresponding allocation is configurable. The device prioritizes non-IP packets according to the priority of the receiving port.

- **untrusted**
  The device ignores the priority information in the data packets and assigns the priority of the receiving port to them.

10.4.3 VLAN tagging

For the VLAN and prioritizing functions, the IEEE 802.1Q standard provides for integrating a MAC frame in the VLAN tag. The VLAN tag consists of 4 bytes and is between the source address field ("Source Address Field") and type field ("Length / Type Field").

![Ethernet data packet with tag](image.png)
For data packets with VLAN tags, the device evaluates the following information:

- Priority information
- When VLANs are configured, VLAN tagging

Data packets with VLAN tags containing priority information but no VLAN information (VLAN ID = 0), are known as Priority Tagged Frames.

**Note:** Network protocols and redundancy mechanisms use the highest traffic class 7. Therefore, select other traffic classes for application data.

When using VLAN prioritizing, consider the following special features:

- End-to-end prioritizing requires the VLAN tags to be transmitted to the entire network. The prerequisite is that every network component is VLAN-capable.
- Routers are not able to send and receive packets with VLAN tags through port-based router interfaces.

### 10.4.4 IP ToS (Type of Service)

The Type-of-Service field (ToS) in the IP header was already part of the IP protocol from the start, and is used to differentiate different services in IP networks. Even back then, there were ideas about differentiated treatment of IP packets, due to the limited bandwidth available and the unreliable connection paths. Because of the continuous increase in the available bandwidth, there was no need to use the ToS field.

Only with the real-time requirements of today's networks has the ToS field become significant again. Selecting the ToS byte of the IP header lets you differentiate between different services. However, this field is not widely used in practice.

<table>
<thead>
<tr>
<th>Bits (0-2): IP Precedence Defined</th>
<th>Bits (3-6): Type of Service Defined</th>
<th>Bit (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>111 - Network Control</td>
<td>0000 - [all normal]</td>
<td>0 - Zero</td>
</tr>
<tr>
<td>110 - Internetwork Control</td>
<td>1000 - [minimize delay]</td>
<td></td>
</tr>
<tr>
<td>101 - CRITIC / ECP</td>
<td>0100 - [maximize throughput]</td>
<td></td>
</tr>
</tbody>
</table>

**Table 21: ToS field in the IP header**
10.4.5 Handling of traffic classes

The device provides the following options for handling traffic classes:

- Strict Priority
- Weighted Fair Queuing
- Strict Priority combined with Weighted Fair Queuing
- Queue management

Strict Priority description

With the Strict Priority setting, the device first transmits data packets that have a higher traffic class (higher priority) before transmitting a data packet with the next highest traffic class. When there are no other data packets remaining in the queue, the device transmits a data packet with the lowest traffic class (lowest priority). In unfortunate cases, if there is a high volume of high-priority traffic waiting to be sent on this port, then the device does not send packets with a low priority.

In delay-sensitive applications, such as VoIP or video, Strict Priority lets data to be sent immediately.

Weighted Fair Queuing description

With Weighted Fair Queuing, also called Weighted Round Robin (WRR), you assign a minimum or reserved bandwidth to each traffic class. This helps ensure that data packets with a lower priority are also sent although the network is very busy.

The reserved values range from 0% through 100% of the available bandwidth, in steps of 1%.

- A reservation of 0 is equivalent to a "no bandwidth" setting.
- The sum of the individual bandwidths can be up to 100%.

When you assign Weighted Fair Queuing to every traffic class, the entire bandwidth of the corresponding port is available to you.

Combining Strict Priority and Weighted Fair Queuing

When combining Weighted Fair Queuing with Strict Priority, verify that the highest traffic class of Weighted Fair Queuing is lower than the lowest traffic class of Strict Priority.

If you combine Weighted Fair Queuing with Strict Priority, then a high Strict Priority network load can significantly reduce the bandwidth available for Weighted Fair Queuing.
10.4.6 Queue management

Defining settings for queue management

Perform the following steps:

- Open the Switching > QoS/Priority > Queue Management dialog.

  The total assigned bandwidth in the Min. bandwidth [%] column is 100%.

- To activate Weighted Fair Queuing for Traffic class = 0, proceed as follows:
  - Unmark the checkbox in the Strict priority column.
  - In the Min. bandwidth [%] column, specify the value 5.

- To activate Weighted Fair Queuing for Traffic class = 1, proceed as follows:
  - Unmark the checkbox in the Strict priority column.
  - In the Min. bandwidth [%] column, specify the value 20.

- To activate Weighted Fair Queuing for Traffic class = 2, proceed as follows:
  - Unmark the checkbox in the Strict priority column.
  - In the Min. bandwidth [%] column, specify the value 30.

- To activate Strict Priority for Traffic class = 3, proceed as follows:
  - Mark the checkbox in the Strict priority column.

- To activate Weighted Fair Queuing for Traffic class = 4, proceed as follows:
  - Unmark the checkbox in the Strict priority column.
  - In the Min. bandwidth [%] column, specify the value 10.

- Save the settings temporarily. To do this, click the button.

```
enable
configure
cos-queue weighted 0

cos-queue min-bandwidth: 0 5

cos-queue weighted 1

cos-queue min-bandwidth: 1 20

cos-queue weighted 2

cos-queue min-bandwidth: 2 30
```

to change to the Privileged EXEC mode.

```
to change to the Configuration mode.
```

to enable Weighted Fair Queuing for traffic class 0.

to assign a weight of 5 % to traffic class 0.

to enable Weighted Fair Queuing for traffic class 1.

to assign a weight of 20 % to traffic class 1.

to enable Weighted Fair Queuing for traffic class 2.

to assign a weight of 30 % to traffic class 2.

```
to show cos-queue
```

<table>
<thead>
<tr>
<th>Queue Id</th>
<th>Min. bandwidth</th>
<th>Scheduler type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
<td>weighted</td>
</tr>
<tr>
<td>1</td>
<td>20</td>
<td>weighted</td>
</tr>
<tr>
<td>2</td>
<td>30</td>
<td>weighted</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>strict</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>strict</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>strict</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>strict</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>strict</td>
</tr>
</tbody>
</table>
10.4.7 Management prioritization

In order for you to constantly have access to the device management, although there is a high network load, the device lets you prioritize management packets.

When prioritizing management packets, the device sends the management packets with priority information.
- On Layer 2, the device modifies the VLAN priority in the VLAN tag. The prerequisite for this function is that the corresponding ports are set to allow sending packets with a VLAN tag.
- On Layer 3, the device modifies the IP-DSCP value.

10.4.8 Setting prioritization

Assigning the port priority

Perform the following steps:

- Open the Switching > QoS/Priority > Port Configuration dialog.
- In the Port priority column, you specify the priority with which the device forwards the data packets received on this port without a VLAN tag.
- In the Trust mode column, you specify the criteria the device uses to assign a traffic class to data packets received.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
configure
interface 1/1
vlan priority 3
exit
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To assign interface 1/1 the port priority 3.
To change to the Configuration mode.

Assigning VLAN priority to a traffic class

Perform the following steps:

- Open the Switching > QoS/Priority > 802.1D/p Mapping dialog.
- To assign a traffic class to a VLAN priority, insert the associated value in the Traffic class column.
- Save the settings temporarily. To do this, click the ✓ button.
Assign port priority to received data packets

Perform the following steps:

```plaintext
enable
configure
classoservice dotlp-mapping 0 2
classoservice dotlp-mapping 1 2
exit
show classoservice dotlp-mapping
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To assign a VLAN priority of 0 to traffic class 2.
To assign a VLAN priority of 1 to traffic class 2.
To change to the Privileged EXEC mode.
To display the assignment.

Assigning DSCP to a traffic class

Perform the following steps:

- Open the Switching > QoS/Priority > IP DSCP Mapping dialog.
- Specify the desired value in the Traffic class column.
- Save the settings temporarily. To do this, click the ✓ button.

```plaintext
enable
configure
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
### Assign the DSCP priority to received IP data packets

Perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>interface 1/1</td>
<td>To change to the interface configuration mode of interface 1/1.</td>
</tr>
<tr>
<td>classofservice trust ip-dscp</td>
<td>To assign the trust ip-dscp mode globally.</td>
</tr>
<tr>
<td>exit</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>show classofservice trust</td>
<td>To display the Trust mode of the ports/interfaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>ip-dscp</td>
</tr>
<tr>
<td>1/2</td>
<td>dot1p</td>
</tr>
<tr>
<td>1/3</td>
<td>dot1p</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>1/5</td>
<td>dot1p</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
</tbody>
</table>

### Configuring Layer 2 management priority

Perform the following steps:

- Open the **Switching > QoS/Priority > Global** dialog.
- In the **VLAN priority for management packets** field, specify the VLAN priority with which the device sends management data packets.
- Save the settings temporarily. To do this, click the ✔️ button.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To assign the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.

To display the priority of the VLAN in which the device management is located.

Perform the following steps:

1. Open the Switching > QoS/Priority > Global dialog.
2. In the IP DSCP value for management packets field, specify the DSCP value with which the device sends management data packets.
3. Save the settings temporarily. To do this, click the ✓ button.

To change to the Privileged EXEC mode.

To assign the DSCP value of 56 to management packets. The device sends management packets with the highest priority.

To display the priority of the VLAN in which the device management is located.
10.5 Flow control

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards surplus data packets.

The flow control mechanism described in standard IEEE 802.3 helps ensure that no data packets are lost due to a port memory overflowing. Shortly before a port memory is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- In half-duplex mode, the device simulates a collision.

The following figure displays how flow control works. Workstations 1, 2, and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2, and 3 is greater than the bandwidth of Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

When the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmission speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming traffic.

![Flow Control Example Diagram](image)

Figure 22: Example of flow control

10.5.1 Halfduplex or fullduplex link

Flow Control with a half duplex link

In the example, there is a halfduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.
Flow Control with a full duplex link

In the example, there is a fullduplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends a request to Workstation 2 to include a small break in the sending transmission.

10.5.2 Setting up the Flow Control

Perform the following steps:

- Open the Switching > Global dialog.
- Mark the Flow control checkbox.
  With this setting you enable flow control in the device.
- Open the Basic Settings > Port dialog, Configuration tab.
- To enable the Flow Control on a port, mark the checkbox in the Flow control column.
- Save the settings temporarily. To do this, click the ✓ button.

Note: When you are using a redundancy function, you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.
11 VLANs

In the simplest case, a virtual LAN (VLAN) consists of a group of network participants in one network segment who can communicate with each other as though they belonged to a separate LAN.

More complex VLANs span out over multiple network segments and are also based on logical (instead of only physical) connections between network participants. VLANs are an element of flexible network design. It is easier to reconfiguring logical connections centrally than cable connections.

The device supports independent VLAN learning in accordance with the IEEE 802.1Q standard which defines the VLAN function.

Using VLANs has many benefits. The following list displays the top benefits:

- **Network load limiting**
  VLANs reduce the network load considerably as the devices transmit Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside the virtual LAN.
  The rest of the data network forwards traffic as normal.
- **Flexibility**
  You have the option of forming user groups based on the function of the participants apart from their physical location or medium.
- **Clarity**
  VLANs give networks a clear structure and make maintenance easier.

11.1 Examples of VLANs

The following practical examples provide a quick introduction to the structure of a VLAN.

**Note:** When configuring VLANs you use an interface for accessing the device management that will remain unchanged. For this example, you use either interface 1/6 or the serial connection to configure the VLANs.
11.1.1 Example 1

The example displays a minimal VLAN configuration (port-based VLAN). An administrator has connected multiple end devices to a transmission device and assigned them to 2 VLANs. This effectively prohibits any data transmission between the VLANs, whose members communicate only within their own VLANs.

When setting up the VLANs, you create communication rules for every port, which you specify in ingress (incoming) and egress (outgoing) tables.

The ingress table specifies which VLAN ID a port assigns to the incoming data packets. Hereby, you use the port address of the end device to assign it to a VLAN.

The egress table specifies on which ports the device sends the packets from this VLAN.

- **T** = Tagged (with a tag field, marked)
- **U** = Untagged (without a tag field, unmarked)

For this example, the status of the TAG field of the data packets has no relevance, so you use the setting **U**.

**Table 22: Ingress table**

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Port</th>
<th>Port VLAN identifier (PVID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 23: Egress table**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>U</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>U</td>
<td></td>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Perform the following steps:

Setting up the VLAN

- Open the Switching > VLAN > Configuration dialog.
- Click the button. The dialog displays the Create window.
- In the VLAN ID field, specify the value 2.
- Click the Ok button.
- For the VLAN, specify the name VLAN2: Double-click in the Name column and specify the name. For VLAN 1, in the Name column, change the value Default to VLAN1.
- Repeat the previous steps to create a VLAN 3 with the name VLAN3.

To change to the Privileged EXEC mode.
To change to the VLAN configuration mode.
To create a new VLAN with the VLAN ID 2.
To assign the name 2 to the VLAN VLAN2.
To create a new VLAN with the VLAN ID 3.
To assign the name 3 to the VLAN VLAN3.
To assign the name 1 to the VLAN VLAN1.
To change to the Privileged EXEC mode.
To display the current VLAN configuration.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>VLAN Type</th>
<th>VLAN Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN1</td>
<td>default</td>
<td>0 days, 00:00:05</td>
</tr>
<tr>
<td>2</td>
<td>VLAN2</td>
<td>static</td>
<td>0 days, 02:44:29</td>
</tr>
<tr>
<td>3</td>
<td>VLAN3</td>
<td>static</td>
<td>0 days, 02:52:26</td>
</tr>
</tbody>
</table>

Setting up the ports

- Open the Switching > VLAN > Configuration dialog.
- To assign the port to a VLAN, specify the desired value in the corresponding column. Possible values:
  - T = The port is a member of the VLAN. The port transmits tagged data packets.
  - U = The port is a member of the VLAN. The port transmits untagged data packets.
  - F = The port is not a member of the VLAN.
  Changes using the GVRP function are disabled.
  - - = The port is not a member of this VLAN.
  Changes using the GVRP function are allowed.
  Because end devices usually interpret untagged data packets, you specify the value U.
- Save the settings temporarily. To do this, click the ✓ button.
- Open the Switching > VLAN > Port dialog.
In the Port-VLAN ID column, specify the VLAN ID of the related VLAN: 2 or 3.

Because end devices usually interpret untagged data packets, in the Acceptable packet types column, you specify the value admitAll for end device ports.

Save the settings temporarily. To do this, click the ✓ button.

The value in the Ingress filtering column has no affect on how this example functions.

```enable
configure
interface 1/1

vlan participation include 2
vlan pvid 2
exit
interface 1/2

vlan participation include 3
vlan pvid 3
exit
interface 1/3

vlan participation include 3
vlan pvid 3
exit
interface 1/4

vlan participation include 2
vlan pvid 2
exit
exit

show vlan id 3
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Current</th>
<th>Configured</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>-</td>
<td>Autodetect</td>
<td>Tagged</td>
</tr>
<tr>
<td>1/2</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/3</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/4</td>
<td>-</td>
<td>Autodetect</td>
<td>Tagged</td>
</tr>
<tr>
<td>1/5</td>
<td>-</td>
<td>Autodetect</td>
<td>Tagged</td>
</tr>
</tbody>
</table>
11.1.2 Example 2

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a 2nd Switch (on the right in the example).

![Diagram of Example 2](image)

**Figure 24: Example of a more complex VLAN configuration**

The terminal devices of the individual VLANs (A to H) are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. If the VLAN is configured correctly, then an optional network management station is also shown, which enables access to every network component.

**Note:** In this case, VLAN 1 has no significance for the end device communication, but it is required for the administration of the transmission devices through what is known as the Management VLAN.

As in the previous example, uniquely assign the ports with their connected terminal devices to a VLAN. With the direct connection between the 2 transmission devices (uplink), the ports transport packets for both VLANs. To differentiate these uplinks you use “VLAN tagging”, which handles the data packets accordingly. Thus, you maintain the assignment to the respective VLANs.

Perform the following steps:

- Add Uplink Port 5 to the ingress and egress tables from example 1.
- Create new ingress and egress tables for the right switch, as described in the first example.

The egress table specifies on which ports the device sends the packets from this VLAN.

| T | Tagged (with a tag field, marked) |
| U | Untagged (without a tag field, unmarked) |

In this example, tagged packets are used in the communication between the transmission devices (Uplink), as packets for different VLANs are differentiated at these ports.

**Table 24: Ingress table for device on left**

<table>
<thead>
<tr>
<th>Terminal</th>
<th>Port</th>
<th>Port VLAN identifier (PVID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Uplink</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
The communication relationships here are as follows: end devices on ports 1 and 4 of the left device and end devices on ports 2 and 4 of the right device are members of VLAN 2 and can thus communicate with each other. The behavior is the same for the end devices on ports 2 and 3 of the left device and the end devices on ports 3 and 5 of the right device. These belong to VLAN 3. The end devices “see” their respective part of the network. Participants outside this VLAN cannot be reached. The device also sends Broadcast, Multicast, and Unicast packets with unknown (unlearned) destination addresses only inside a VLAN.

Here, the devices use VLAN tagging (IEEE 801.1Q) within the VLAN with the ID 1 (Uplink). The letter T in the egress table of the ports indicates VLAN tagging.

The configuration of the example is the same for the device on the right. Proceed in the same way, using the ingress and egress tables created above to adapt the previously configured left device to the new environment.

Perform the following steps:
- Setting up the VLAN
  - Open the **Switching > VLAN > Configuration** dialog.
  - Click the button. The dialog displays the Create window.
  - In the VLAN ID field, specify the VLAN ID, for example 2.
Click the **Ok** button.

For the VLAN, specify the name **VLAN2**:
- Double-click in the **Name** column and specify the name. 
  For **VLAN 1**, in the **Name** column, change the value **Default** to **VLAN1**.

Repeat the previous steps to create a VLAN **3** with the name **VLAN3**.

---

**enable**

**vlan database**

**vlan add 2**

name **2 VLAN2**

**vlan add 3**

name **3 VLAN3**

name **1 VLAN1**

**exit**

**show vlan brief**

---

Max. VLAN ID: **4042**

Max. supported VLANs: **128**

Number of currently configured VLANs: **3**

VLAN unaware mode: **disabled**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>VLAN Type</th>
<th>VLAN Creation Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN1</td>
<td>default</td>
<td>0 days, 00:00:05</td>
</tr>
<tr>
<td>2</td>
<td>VLAN2</td>
<td>static</td>
<td>0 days, 02:44:29</td>
</tr>
<tr>
<td>3</td>
<td>VLAN3</td>
<td>static</td>
<td>0 days, 02:52:26</td>
</tr>
</tbody>
</table>

---

Open the **Switching > VLAN > Configuration** dialog.

To assign the port to a VLAN, specify the desired value in the corresponding column. Possible values:
- **T** = The port is a member of the VLAN. The port transmits tagged data packets.
- **U** = The port is a member of the VLAN. The port transmits untagged data packets.
- **F** = The port is not a member of the VLAN.
- **-** = The port is not a member of this VLAN.

Changes using the **GVRP** function are disabled.

Because end devices usually interpret untagged data packets, you specify the value **U**. You specify the **T** setting on the uplink port on which the VLANs communicate with each other.

Save the settings temporarily. To do this, click the **✓** button.

Open the **Switching > VLAN > Port** dialog.

In the **Port-VLAN ID** column, specify the VLAN ID of the related VLAN:
- **1**, **2** or **3**

Because end devices usually interpret untagged data packets, in the **Acceptable packet types** column, you specify the value **admitAll** for end device ports.
For the uplink port, in the *Acceptable packet types* column, specify the value `admitOnlyVlanTagged`.

Mark the checkbox in the *Ingress filtering* column for the uplink ports to evaluate VLAN tags on this port.

Save the settings temporarily. To do this, click the ✅ button.

```plaintext
enable
cfg
inter 1/1
vlp i 1
vlp i 2
vlte 2
vlp i 3
vlte 3
vlid 1
vlisf
vlaf v1only
ex
inter 1/2
vlp i 2
ex
inter 1/3
vlp i 3
ex
inter 1/4
vlp i 2
ex
inter 1/5
vlp i 3
vlid 3
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/1.

The port 1/1 becomes a member of the VLAN 1 and transmits the data packets without a VLAN tag.

The port 1/1 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.

The port 1/1 becomes a member of the VLAN 2 and transmits the data packets with a VLAN tag.

The port 1/1 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.

The port 1/1 becomes a member of the VLAN 3 and transmits the data packets with a VLAN tag.

To assign the Port VLAN ID 1 to port 1/1.

To activate ingress filtering on port 1/1.

Port 1/1 only forwards packets with a VLAN tag.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/2.

The port 1/2 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.

To assign the Port VLAN ID 2 to port 1/2.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/3.

The port 1/3 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.

To assign the Port VLAN ID 3 to port 1/3.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/4.

The port 1/4 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.

To assign the Port VLAN ID 2 to port 1/4.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/5.

The port 1/5 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.

To assign the Port VLAN ID 3 to port 1/5.
**VLAN ID**......................3
**VLAN Name**..................VLAN3
**VLAN Type**...............Static
**VLAN Creation Time**.......0 days, 00:07:47 (System Uptime)
**VLAN Routing**.............disabled

<table>
<thead>
<tr>
<th>Interface</th>
<th>Current</th>
<th>Configured</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Include</td>
<td>Include</td>
<td>Tagged</td>
</tr>
<tr>
<td>1/2</td>
<td>-</td>
<td>Autodetect</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/3</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/4</td>
<td>-</td>
<td>Autodetect</td>
<td>Untagged</td>
</tr>
<tr>
<td>1/5</td>
<td>Include</td>
<td>Include</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

To change to the Configuration mode.
To change to the Privileged EXEC mode.
To display details for VLAN 3.
11.2 Guest VLAN / Unauthenticated VLAN

A Guest VLAN lets a device provide port-based Network Access Control (IEEE 802.1x) to non-802.1x capable supplicants. This feature provides a mechanism to allow guests to access external networks only. If you connect non-802.1x capable supplicants to an active unauthorized 802.1x port, then the supplicants send no responses to 802.1x requests. Since the supplicants send no responses, the port remains in the unauthorized state. The supplicants have no access to external networks.

The Guest VLAN supplicant is a per-port basis configuration. When you configure a port as a Guest VLAN and connect non-802.1x capable supplicants to this port, the device assigns the supplicants to the Guest VLAN. Adding supplicants to a Guest VLAN causes the port to change to the authorized state allowing the supplicants to access to external networks.

An Unauthenticated VLAN lets the device provide service to 802.1x capable supplicants which authenticate incorrectly. This function lets the unauthorized supplicants have access to limited services. If you configure an Unauthenticated VLAN on a port with 802.1x port authentication and the global operation enabled, then the device places the port in an Unauthenticated VLAN. When a 802.1x capable supplicant incorrectly authenticates on the port, the device adds the supplicant to the Unauthenticated VLAN. If you also configure a Guest VLAN on the port, then non-802.1x capable supplicants use the Guest VLAN.

If the port has an Unauthenticated VLAN assigned, then the reauthentication timer counts down. When the time specified in the Reauthentication period [s] column expires and supplicants are present on the port, the Unauthenticated VLAN reauthenticates. When no supplicants are present, the device places the port in the configured Guest VLAN.

The following example explains how to create a Guest VLAN. Create an Unauthorized VLAN in the same manner.

Perform the following steps:

- Open the Switching > VLAN > Configuration dialog.
- Click the button.
  The dialog displays the Create window.
- In the VLAN ID field, specify the value 10.
- Click the Ok button.
- For the VLAN, specify the name Guest:
  Double-click in the Name column and specify the name.
- Click the button.
  The dialog displays the Create window.
- In the VLAN ID field, specify the value 20.
- Click the Ok button.
- For the VLAN, specify the name Not authorized:
  Double-click in the Name column and specify the name.
- Open the Network Security > 802.1X > Global dialog.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
Open the Network Security > 802.1X > Port Configuration dialog.

Specify the following settings for port 1/4:
- The value `auto` in the Port control column
- The value `10` in the Guest VLAN ID column
- The value `20` in the Unauthenticated VLAN ID column

Save the settings temporarily. To do this, click the ✓ button.

```
enable
vlan database
vlan add 10
vlan add 20
name 10 Guest
name 20 Unauth
exit
configure
dot1x system-auth-control enable
dot1x port-control auto
interface 1/4
dot1x guest-vlan 10
dot1x unauthenticated-vlan 20
exit
```

To change to the Privileged EXEC mode.
To change to the VLAN configuration mode.
To create VLAN 10.
To create VLAN 20.
To rename VLAN 10 to Guest.
To rename VLAN 20 to Unauth.
To change to the Privileged EXEC mode.
To change to the Configuration mode.
To enable the 802.1X function globally.
To enable port control on port 1/4.
To change to the interface configuration mode of interface 1/4.
To assign the guest vlan to port 1/4.
To assign the unauthorized vlan to port 1/4.
To change to the Configuration mode.
11.3  RADIUS VLAN assignment

The RADIUS VLAN assignment feature makes it possible for a RADIUS VLAN ID attribute to be associated with an authenticated client. When a client authenticates successfully, and the RADIUS server sends a VLAN attribute, the device associates the client with the RADIUS assigned VLAN. As a result, the device adds the physical port as an member to the appropriate VLAN and sets the port VLAN ID (PVID) with the given value. The port transmits the data packets without a VLAN tag.
11.4 Creating a Voice VLAN

Use the Voice VLAN feature to separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to safeguard the sound quality of an IP phone in cases where there is high data traffic on the port.

The device uses the source MAC address to identify and prioritize the voice data flow. Using a MAC address to identify devices helps prevent a rogue client from connecting to the same port causing the voice traffic to deteriorate.

Another benefit of the Voice VLAN feature is that a VoIP phone obtains a VLAN ID or priority information using LLDP-MED. As a result, the VoIP phone sends voice data as tagged, priority tagged or untagged. This depends on the Voice VLAN Interface configuration.

The following Voice VLAN interface modes are possible. The first 3 methods segregate and prioritize voice and data traffic. Traffic segregation results in an increased voice traffic quality during high traffic periods.

- Configuring the port to use the `vlan` mode lets the device tag the voice data coming from a VoIP phone with the user-defined voice VLAN ID. The device assigns regular data to the default port VLAN ID.
- Configuring the port to use the `dot1p-priority` mode lets the device tag the data coming from a VoIP phone with VLAN 0 and the user-defined priority. The device assigns the default priority of the port to regular data.
- Configure both the voice VLAN ID and the priority using the `vlan/dot1p-priority` mode. In this mode the VoIP phone sends voice data with the user-defined voice VLAN ID and priority information. The device assigns the default PVID and priority of the port to regular data.
- When configured as `untagged`, the phone sends untagged packets.
- When configured as `none`, the phone uses its own configuration to send voice traffic.
VLANs

11.5 VLAN unaware mode

The **VLAN-unaware mode** defines the operation of the device in a LAN segmented by VLANs. The device accepts packets and processes them according to its inbound rules. Based on the IEEE 802.1Q specifications, the function governs how the device processes VLAN tagged packets.

Use the VLAN aware mode to apply the user-defined VLAN topology configured by the network administrator. When the device forwards packets, it uses VLAN tagging in combination with the IP or Ethernet address. The device processes inbound and outbound packets according to the defined rules. VLAN configuration is a manual process.

Use the VLAN unaware mode to forward traffic as received, without any modification. When the device receives packets as tagged, it transmits tagged packets. When the device receives packets as untagged, it transmits untagged packets. Regardless of VLAN assignment mechanisms, the device assigns packets to VLAN ID 1 and to a Multicast group, indicating that the packet flood domain is according to the VLAN.
12 Redundancy

12.1 Network Topology vs. Redundancy Protocols

When using Ethernet, a significant prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:
- Line topology
- Star topology
- Tree topology

![Figure 25: Network with line, star and tree topologies](image)

To maintain communication in case a connection failure is detected, install additional physical connections between the network nodes. Redundancy protocols help ensure that the additional connections remain switched off while the original connection is still working. When a connection failure is detected, the redundancy protocol generates a new path from the sender to the receiver through the alternative connection.

To introduce redundancy onto Layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

12.1.1 Network topologies

Meshed topology

For networks with star or tree topologies, redundancy procedures are only possible in connection with physical loop creation. The result is a meshed topology.

![Figure 26: Meshed topology: Tree topology with physical loops](image)
For operating in this network topology, the device provides you with the following redundancy protocols:

- Rapid Spanning Tree (RSTP)

### Ring topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This creates a ring topology.

![Figure 27: Ring topology: Line topology with connected ends](image)

For operating in this network topology, the device provides you with the following redundancy protocols:

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

### 12.1.2 Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

**Table 28: Overview of redundancy protocols**

<table>
<thead>
<tr>
<th>Redundancy protocol</th>
<th>Network topology</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRP</td>
<td>Ring</td>
<td>The switching time can be selected and is practically independent of the number of devices. An MRP Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you only use Hirschmann devices, up to 100 devices are possible in the MRP Ring.</td>
</tr>
<tr>
<td>Sub Ring</td>
<td>Ring</td>
<td>The <em>Sub Ring</em> function lets you easily couple network segments to existing redundancy rings.</td>
</tr>
</tbody>
</table>
| RSTP                | Random structure | The switching time depends on the network topology and the number of devices.  
|                     |                  | - typ. < 1 s with RSTP  
|                     |                  | - typ. < 30 s with STP |
| Link Aggregation    | Random structure | A Link Aggregation Group (LAG) is a combination of 2 or more links between 2 switches to increase bandwidth. Each involved link operates in full-duplex mode and with the same data rate. |
| Link Backup         | Random structure | When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks. |

**Note:** If you are using a redundancy function, then you deactivate the flow control on the participating device ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.
12.1.3 **Combinations of redundancy protocols**

*Table 29: Overview of redundancy protocol combinations*

<table>
<thead>
<tr>
<th></th>
<th>MRP</th>
<th>RSTP</th>
<th>Link Aggreg.</th>
<th>Link Backup</th>
<th>Sub Ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRP</td>
<td>▲</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>RSTP</td>
<td>▲ 1)</td>
<td>▲</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Link Aggreg.</td>
<td>▲ 2)</td>
<td>▲ 2)</td>
<td>▲</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Link Backup</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>▲</td>
<td>—</td>
</tr>
<tr>
<td>Sub Ring</td>
<td>▲</td>
<td>▲</td>
<td>▲ 2)</td>
<td>▲</td>
<td>▲</td>
</tr>
</tbody>
</table>

▲ Combination applicable
○ Combination not applicable

1) A redundant coupling between these network topologies will possibly lead to loops.
2) Combination applicable on the same port
12.2 Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

An MRP Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you only use Hirschmann devices, up to 100 devices are possible in the MRP Ring.

When you use the fixed MRP redundant port (Fixed Backup) and a primary ring link failure is detected, the Ring Manager forwards data to the secondary ring link. When the primary link is restored, the secondary link continues to be in use.

12.2.1 Network Structure

The concept of ring redundancy lets you construct high-availability ring-shaped network structures.

With the help of the RM (Ring Manager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The Ring Manager keeps the redundant line open as long as the line structure is intact. When a segment becomes inoperable, the Ring Manager immediately closes the redundant line, and line structure is intact again.

![Line structure](image)

*Figure 28: Line structure*

![Redundant ring structure](image)

*Figure 29: Redundant ring structure*

RM = Ring Manager
--- main line
- - - redundant line
12.2.2 Reconfiguration time

When a line section failure is detected, the Ring Manager changes the MRP Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the Ring Manager.

Possible values for the maximum delay time:
- 500ms
- 30ms

Note: If every device in the ring supports the shorter delay time, then you can configure the reconfiguration time with a value less than 500ms.

Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

12.2.3 Advanced mode

For times even shorter than the specified reconfiguration times, the device provides the advanced mode. When the ring participants inform the Ring Manager of interruptions in the ring through link-down notifications, the advanced mode speeds up the link failure recognition.

Hirschmann devices support link-down notifications. Therefore, you generally activate the advanced mode in the Ring Manager.

When you are using devices that do not support link-down notifications, the Ring Manager reconfigures the line in the selected maximum reconfiguration time.

12.2.4 Prerequisites for MRP

Before setting up an MRP Ring, verify that the following conditions are fulfilled:
- All ring participants support MRP.
- The ring participants are connected to each other through the ring ports. Apart from its neighbors, no other ring participants are connected to the respective device.
- All ring participants support the configuration time specified in the Ring Manager.
- There is only one Ring Manager in the ring.

If you are using VLANs, then configure every ring port with the following settings:
- Deactivate ingress filtering - see the Switching > VLAN > Port dialog.
- Define the port VLAN ID (PVID) - see the Switching > VLAN > Port dialog.
  - PVID = 1 in cases where the device transmits the MRP data packets untagged (VLAN ID = 0 in Switching > L2-Redundancy > MRP dialog)
    By setting the PVID = 1, the device automatically assigns the received untagged packets to VLAN 1.
  - PVID = any in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥1 in the Switching > L2-Redundancy > MRP dialog)
- Define egress rules - see Switching > VLAN > Configuration dialog.
  - U (untagged) for the ring ports of VLAN 1 in cases where the device transmits the MRP data packets untagged (VLAN ID = 0 in the Switching > L2-Redundancy > MRP dialog, the MRP Ring is not assigned to a VLAN).
  - T (tagged) for the ring ports of the VLAN which you assign to the MRP Ring. Select T, in cases where the device transmits the MRP data packets in a VLAN (VLAN ID ≥1 in the Switching > L2-Redundancy > MRP dialog).
12.2.5 Advanced Information

MRP Packets

MRP uses test packets, link-change packets, and topology-change packets (FDB flush packets).

The Ring Manager (RM) is connected to the ring with 2 ring ports. As long as all connections in the ring are operational, the RM sets one of its ports, the redundant port, into the blocking state. In this state, the redundant port neither receives nor sends normal (payload) data packets. This way, the RM prevents a network loop.

The RM periodically sends test packets into the ring from both ring ports. The test packets are special packets. The RM sends and receives test packets even at the redundant port although the redundant port blocks normal packets. The RM expects to receive the test packets on its respective other ring port. If the RM does not receive any expected test packets for a specified amount of time, the RM detects a ring failure.

If the Advanced mode function is active, the RM also reacts to link-down packets from ring devices. The prerequisite is that each ring device supports the sending of link-change packets to the RM when a link between 2 ring devices goes down or up. These packets help the RM to react more quickly to a link failure or recovery. The RM receives the link-change packets even on its redundant port.

On reconfiguration of the ring, the RM flushes its Forwarding Database (FDB) and sends topology-change packets to the ring devices. The topology-change packets prompt the ring devices to flush their FDB, too. This procedure helps forward the payload packets over the new path more quickly. This procedure is performed regardless whether the ring reconfiguration was caused by a link-down or a link-up.

Table 30: MRP Packets

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Send Mode</th>
<th>Time Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test packet¹</td>
<td>Periodically</td>
<td>Send interval</td>
<td>50 ms (for ring recovery time 500 ms)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20 ms (for ring recovery time 200 ms)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reception timeout</td>
<td>400 ms (for ring recovery time 500 ms)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>160 ms (for ring recovery time 200 ms)</td>
</tr>
<tr>
<td>Link-down packet²</td>
<td>Event-driven</td>
<td>On link-down of a ring port</td>
<td>-</td>
</tr>
<tr>
<td>Topology-change packet³</td>
<td>Event-driven</td>
<td>On reconfiguration</td>
<td>-</td>
</tr>
</tbody>
</table>

1. Sent by the Ring Manager only.
2. Sent by supporting ring participants.
3. The reception of a topology-change packet prompts the supporting ring devices to flush their FDB.
**MRP Packet Prioritization**

The ring devices send the MRP test packets, the link-change packets, and the topology-change packets with a user-configurable VLAN ID. The default VLAN ID is 0. The devices send the test packets untagged and thus without priority (Class of Service) information.

To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The devices then send and forward these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize the test packets, perform the following steps on the Ring Manager and on the ring devices:
- Specify the MRP VLAN ID to a value ≥ 1.
- Specify the ring ports as T (tagged) members of this MRP VLAN ID.

**Note:** When you set the MRP VLAN ID to a value ≥ 1 in the Switching > L2-Redundancy > MRP dialog, the device adds its ring ports as T (tagged) members of this MRP VLAN ID. If the MRP VLAN does not yet exist, the device automatically creates this VLAN. After setting a new MRP VLAN ID, check the Switching > VLAN > Configuration dialog for the VLAN and the port settings.

### 12.2.6 Example Configuration

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used. All devices support MRP. On every device you define ports 1.1 and 1.2 as ring ports.

When a primary ring link failure is detected, the Ring Manager sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.

![Figure 30: Example of MRP Ring](image)

RM = Ring Manager

--- main line

- - redundant line

The following example configuration describes the configuration of the Ring Manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without enabling the Ring manager function. This example does not use a VLAN. You specify the value 30 ms as the ring recovery time. Every device supports the advanced mode of the Ring Manager.

- Set up the network to meet your demands.
- To minimize the ring recovery time in case of a link-up after a failure, configure the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually configure 100 Mbit/s Full Duplex (FDX).
  - For the other port types, keep the port-specific default settings.
**Note:** Configure each device of the MRP Ring individually. Before you connect the redundant line, verify that you have completed the configuration of every device of the MRP Ring. You thus help avoid loops during the configuration phase.

You deactivate the flow control on the participating ports.

If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended. (Default setting: flow control deactivated globally and activated on every port.)

Disable the *Spanning Tree* function in every device in the network. To do this, perform the following steps:

- Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- Disable the function.
  
  In the state on delivery, Spanning Tree is enabled in the device.

- **enable**
- **configure**
- **no spanning-tree operation**
- **show spanning-tree global**

Enable MRP on every device in the network. To do this, perform the following steps:

- Open the *Switching > L2-Redundancy > MRP* dialog.
- Specify the desired ring ports.

In the Command Line Interface you first define an additional parameter, the MRP domain ID. Configure every ring participant with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the Graphical User Interface, the device uses the default value `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

- **mrp domain add default-domain**
  
  To create a new MRP domain with the ID `default-domain`.

- **mrp domain modify port primary 1/1**
  
  To specify port `1/1` as ring port `1`.

- **mrp domain modify port secondary 1/2**
  
  To specify port `1/2` as ring port `2`. 

Enable the **Fixed backup** port. To do this, perform the following steps:

- Enable the Ring Manager.  
  For the other devices in the ring, leave the setting as **Off**.

- To allow the device to continue sending data on the secondary port after the ring is restored, mark the **Fixed backup** checkbox.

  **Note:** When the device reverts back to the primary port, the maximum ring recovery time can be exceeded.

  When you unmark the **Fixed backup** checkbox, and the ring is restored, the Ring Manager blocks the secondary port and unblocks the primary port.

```
mrp domain modify port secondary 1/2 fixed-backup enable
```

To activate the **Fixed backup** function on the secondary port. The secondary port continues forwarding data after the ring is restored.

- Enable the Ring Manager.  
  For the other devices in the ring, leave the setting as **Off**.

```
mrp domain modify mode manager
```

To specify that the device operates as the **Ring manager**. For the other devices in the ring, leave the default setting.

- Select the checkbox in the **Advanced mode** field.

```
mrp domain modify advanced-mode enabled
```

To activate the advanced mode.

- In the **Ring recovery** field, select the value **30ms**.

```
mrp domain modify recovery-delay 200ms
```

To specify the value **30ms** as the max. delay time for the reconfiguration of the ring.

**Note:** If selecting the value **30ms** for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, then select the value **500ms**.

- Switch the operation of the MRP Ring on.

- Save the settings temporarily. To do this, click the **✓** button.

```
mrp domain modify operation enable
```

To activate the MRP Ring.
When every ring participant is configured, close the line to the ring. To do this, you connect the devices at the ends of the line through their ring ports.

Check the messages from the device. To do this, perform the following steps:

- show mrp  
  To display the parameters for checking.

The **Operation** field displays the operating state of the ring port.

Possible values:
- **forwarding**  
  The port is enabled, connection exists.
- **blocked**  
  The port is blocked, connection exists.
- **disabled**  
  The port is disabled.
- **not-connected**  
  No connection exists.

The **Information** field displays messages for the redundancy configuration and the possible causes of detected errors.

When the device is operating as a ring client or a Ring Manager, the following messages are possible:
- **Redundancy available**  
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- **Configuration error: Error on ringport link.**  
  An error is detected in the cabling of the ring ports.

When the device is operating as a Ring Manager, the following messages are possible:
- **Configuration error: Packets from another ring manager received.**  
  Another device exists in the ring that is operating as the Ring Manager. Enable the **Ring manager** function on exactly one device in the ring.
- **Configuration error: Ring link is connected to wrong port.**  
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one ring port.

When applicable, integrate the MRP Ring into a VLAN. To do this, perform the following steps:

- In the **VLAN ID** field, define the MRP VLAN ID. The MRP VLAN ID determines in which of the configured VLANs the device transmits the MRP packets.
  To set the MRP VLAN ID, first configure the VLANs and the corresponding egress rules in the **Switching > VLAN > Configuration** dialog.
  - If the MRP Ring is not assigned to a VLAN (like in this example), then leave the VLAN ID as 0.
    In the **Switching > VLAN > Configuration** dialog, specify the VLAN membership as U (untagged) for the ring ports in VLAN 1.
  - If the MRP Ring is assigned to a VLAN, then enter a VLAN ID >0.  
    In the **Switching > VLAN > Configuration** dialog, specify the VLAN membership as T (tagged) for the ring ports in the selected VLAN.

- mrp domain modify vlan  <0..4042>  
  To assign the VLAN ID.
12.2.7 MRP over LAG

Hirschmann devices allow you to combine Link Aggregation Groups (LAG) to increase bandwidth with the Media Redundancy Protocol (MRP) providing redundancy. The function lets you increase the bandwidth on individual segments or on the entire network.

The Link Aggregation function helps you overcome bandwidth limitations of individual ports. LAG lets you combine 2 or more links in parallel, creating one logical link between 2 devices. The parallel links increase the bandwidth for the data stream between the 2 devices.

An MRP Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. When you use only Hirschmann devices, the protocol lets you configure MRP Rings with up to 100 devices.

You use MRP over LAG in the following cases:
- to increase bandwidth only on specific segments of an MRP Ring
- to increase bandwidth on the entire MRP Ring

Network Structure

When configuring an MRP Ring with LAGs, the Ring Manager (RM) monitors both ends of the backbone for continuity. The RM blocks data on the secondary (redundant) port as long as the backbone is intact. When the RM detects an interruption of the data stream on the ring, it begins forwarding data on the secondary port, which restores backbone continuity.

You use LAG instances in MRP Rings to increase bandwidth only, in this case MRP provides the redundancy.

In order for the RM to detect an interruption on the ring, MRP requires a device to block every port in the LAG instance in cases where a port in the instance is down.

LAG on a single segment of an MRP Ring

The device lets you configure a LAG instance on specific segments of an MRP Ring.

You use the LAG Single Switch method for devices in the MRP Ring. The Single Switch method provides you an inexpensive way to grow your network by using only one device on each side of a segment to provide the physical ports. You group the ports of the device into a LAG instance to provide increased bandwidth on specific segments where needed.

![Link Aggregation over a single link of an MRP Ring](image-url)
LAG on an entire MRP Ring

Besides being able to configure a LAG instance on specific segments of an MRP Ring, Hirschmann devices also allow you to configure LAG instances on every segment, which increases bandwidth on the entire MRP Ring.

![Figure 32: Link Aggregation over the entire MRP Ring.](image)

Detecting interruptions on the ring

When configuring the LAG instance, specify the Active ports (min.) value to equal the total number of ports used in the LAG instance. When a device detects an interruption on a port in the LAG instance, it blocks data on the other ports of the instance. With every port of an instance blocked, the RM senses that the ring is open and begins forwarding data on the secondary port. This way the RM is able to restore continuity to the devices on the other side of the interrupted segment.

![Figure 33: Interruption of a link in an MRP Ring](image)
**Example Configuration**

In the following example, switch A and switch B link two departments. The departments produce traffic too high for the individual port bandwidth to handle. You configure a LAG instance for the single segment of the MRP Ring, increasing the bandwidth of the segment.

The prerequisite for the example configuration is that you begin with an operational MRP Ring.

![MRP over LAG Configuration Example](image)

Configure switch A first. To do this, perform the following steps. Then configure switch B using the same steps, substituting the appropriate port and ring port numbers.

1. Open the **Switching > L2-Redundancy > Link Aggregation** dialog.
2. Click the **+** button.  
   The dialog displays the **Create** window.
3. From the **Trunk port** drop-down list, select the instance number of the link aggregation group.
4. From the **Port** drop-down list, select port **1/1**.
5. Click the **Ok** button.
6. Repeat the preceding steps and select the port **1/2**.
7. Click the **Ok** button.
8. In the **Active ports (min.)** column enter **2**, which in this case is the total number of ports in the instance. When combining MRP and LAG you specify the total number of ports as the **Active ports (min.)**. When the device detects an interruption on a port, it blocks the other ports in the instance causing the ring to open. The Ring Manager senses that the ring is open, then begins forwarding data on its secondary ring port which restores the connectivity to the other devices in the network.
9. Save the settings temporarily. To do this, click the **✓** button.
10. Open the **Switching > L2-Redundancy > MRP** dialog.
11. In the **Ring port 2** frame, select port **lag/1** from the **Port** drop-down list.
12. Save the settings temporarily. To do this, click the **✓** button.

```
enable
configure
link-aggregation add lag/1
link-aggregation modify lag/1 addport 1/1
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a Link Aggregation Group **lag/1**.
To add port **1/1** to the Link Aggregation Group.
Redundancy
12.2 Media Redundancy Protocol (MRP)

- `link-aggregation modify lag/1 addport 1/2`
  To add port 1/2 to the Link Aggregation Group.

- `mrp domain modify port secondary lag/1`
  To specify port lag/1 as ring port 2.

- `copy config running-config nvm`
  To save the current settings in the non-volatile memory (nvm) in the “selected” configuration profile.
12.3 Spanning Tree

**Note:** The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for the device.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus interruption of communication across the network. In order to help avoid this, you can use Spanning Tree. Spanning Tree helps avoid loops through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. When a connection or a bridge becomes inoperable, the STP requires a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

**Note:** RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the devices takes over the role of the root bridge here. The maximum number of devices permitted in an active branch from the root bridge to the tip of the branch is specified by the variable `Max age` for the current root bridge. The preset value for `Max age` is 20, which can be increased up to 40.

If the device working as the root is inoperable and another device takes over its function, then the `Max age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

**Note:** The RSTP standard requires that every device within a network operates with the (Rapid) Spanning Tree Algorithm. When STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.

A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the Common Spanning Tree (CST).

12.3.1 Basics

Because RSTP is a further development of the STP, every of the following descriptions of the STP also apply to RSTP.
The tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. When a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This lets redundant links increase the availability of communication.

STP determines a bridge that represents the STP tree structure’s base. This bridge is called root bridge.

Features of the STP algorithm:
- automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
- the tree structure is stabilized up to the maximum network size,
- stabilization of the topology within a short time period
- topology can be specified and reproduced by the administrator
- transparency for the end devices
- low network load relative to the available transmission capacity due to the tree structure created

Bridge parameters

In the context of Spanning Tree, each bridge and its connections are uniquely described by the following parameters:
- Bridge Identifier
- Root Path Cost for the bridge ports,
- Port Identifier

Bridge Identifier

The Bridge Identifier consists of 8 bytes. The bridge with the smallest number for the Bridge Identifier has the highest bridge priority.

According to the original standard IEEE 802.1D-1998, the 2 highest-value bytes are the Bridge Priority. When configuring the bridge, the bridge administrator can change the default setting for the Bridge Priority which is \texttt{32768} (8000H).

In the newer standard IEEE 802.1Q-2014, the Bridge Priority is interpreted differently. The highest 4 bits represent the Bridge Priority. The lower 12 bits are reserved for the VLAN ID and are all zero. As a consequence, the bridge administrator can set the Bridge Priority in steps of 4096. The default value is \texttt{32768} (8000H), and the max. value is \texttt{61440} (F000H).

The 6 lowest-value bytes of the Bridge Identifier are the MAC address of the bridge. The MAC address lets each bridge have a unique Bridge Identifier.

![Bridge Identifier, Example (interpretation according to IEEE 802.1D-1998, values in hexadecimal notation)](image)
Root Path Cost

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The device determines this value based on the transmission speed (see table 31 on page 187). The device assigns a higher path cost to paths with lower transmission speeds.

Alternatively, the Administrator can set the path cost. Like the device, the Administrator assigns a higher path cost to paths with lower transmission speeds. However, since the Administrator can choose this value freely, he has a tool with which he can give a certain path an advantage among redundant paths.

The root path cost is the sum of the individual costs of those paths that a data packet has to traverse from a connected bridge’s port to the root bridge.

![Figure 36: Path costs](image)

Table 31: Recommended path costs for RSTP based on the data rate.

<table>
<thead>
<tr>
<th>Data rate</th>
<th>Recommended value</th>
<th>Recommended range</th>
<th>Possible range</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤100 kbit/s</td>
<td>20 000 000(^1)</td>
<td>20 000 000-200 000 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>1 Mbit/s</td>
<td>20 000 000(^a)</td>
<td>20 000 000-200 000 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>10 Mbit/s</td>
<td>20 000 000(^a)</td>
<td>20 000 000-200 000 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>100 Mbit/s</td>
<td>20 000 000(^a)</td>
<td>20 000 000-200 000 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>1 Gbit/s</td>
<td>20 000</td>
<td>2 000-20 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>10 Gbit/s</td>
<td>200</td>
<td>20-2 000</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>100 Gbit/s</td>
<td>20</td>
<td>2-20</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>1 TBit/s</td>
<td>2</td>
<td>1-20</td>
<td>1-200 000 000</td>
</tr>
<tr>
<td>10 TBit/s</td>
<td>2</td>
<td>1-20</td>
<td>1-200 000 000</td>
</tr>
</tbody>
</table>

\(^1\) Verify that bridges, which conform to IEEE 802.1D-1998 and only support 16-bit values for the path costs, use the value 65535 (FFFFH) for path costs in cases where they are used in conjunction with bridges that support 32-bit values for the path costs.
**Port Identifier**

According to the original standard IEEE 802.1D-1998, the Port Identifier consists of 2 bytes. The lower-value byte contains the physical port number. This provides a unique identifier for the port of this bridge. The higher-value byte is the Port Priority, which is specified by the Administrator (default value: 128 or 80H).

In the newer standard IEEE 802.1Q-2014, the Port Priority is interpreted differently. The highest 4 bits represent the Port Priority. The lower 12 bits are the port number. This allows for bridges with up to 4095 ports. As a consequence, the bridge administrator can set the Port Priority in steps of 4096, when viewed as a 16-bit number. The default value is 32768 (8000H), and the max. value is 61440 (F000H). When viewed as 4-bit number, the default value is 8 (8H), the min. value is 0 (0H), and the max. value is 15 (FH).

![Port Identifier (interpretation according to IEEE 802.1D-1998)](image)

**Max Age and Diameter**

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

**Diameter**

The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.

![Definition of diameter](image)

The network diameter that can be achieved in the network is MaxAge-1.

In the state on delivery, MaxAge = 20 and the maximum diameter that can be achieved = 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved = 39.
MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.

Before forwarding a STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value specified in the device:
- When MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- When MessageAge = MaxAge, the bridge discards the STP-BPDU.

12.3.2 Rules for Creating the Tree Structure

Bridge information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.

To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include:
- Bridge identifier
- Root path costs
- Port identifier

(see IEEE 802.1D)
Setting up the tree structure

The bridge with the smallest number for the bridge identifier is called the root bridge. It is (or will become) the root of the tree structure.

The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge become as small as possible.

- When there are multiple paths with the same root path costs, the bridge further away from the root decides which port it blocks. For this purpose, it uses the bridge identifiers of the bridge closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is the logically worse one). When 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
- When multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further away from the root uses the port identifier of the other bridge as the last criterion (see figure 37 on page 188). In the process, the bridge blocks the port that leads to the port with the numerically higher ID. A numerically higher ID is the logically worse one. When 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.

Figure 40: Flow diagram for specifying the root path
12.3.3 Examples

Example of determining the root path

You can use the network plan to follow the flow chart (see figure 40 on page 190) for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example every sub-path has the same path costs. The protocol blocks the path between bridge 2 and bridge 3 because a connection from bridge 3 through bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:
- The path through bridge 5 and bridge 3 creates the same root path costs as the path through bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4. The port identifier is decisive here (Port 1 < Port 3).

![Figure 41: Example of a network plan for determining the root path](image)

Note: When the current root bridge goes down, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge, because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge.
Example of manipulating the root path

You can use the network plan to follow the flow chart (see figure 40 on page 190) for determining the root path. The Administrator has performed the following:

- Left the default value of 32768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- assigned to bridge 1 the value 16384 (4000H), thus making it the root bridge.
- To bridge 5 he assigned the value 28672 (7000H).

The protocol blocks the path between bridge 2 and bridge 3 because a connection from bridge 3 through bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- The bridges select the path through bridge 5 because the value 28672 for the priority in the bridge identifier is smaller than value 32768.

Figure 42: Example of a network plan for manipulating the root path
Example of manipulating the tree structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to every other bridge add up.

When the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown in the following figure. The path costs for most of the bridges to the root bridge have decreased.

Figure 43: Example of manipulating the tree structure
12.4 Rapid Spanning Tree Protocol

RSTP uses the same algorithm for determining the tree structure as STP. When a link or bridge becomes inoperable, RSTP adds mechanisms that speed up the reconfiguration.

The ports play a significant role in this context.

12.4.1 Port roles

RSTP assigns each bridge port one of the following roles:

- **Root Port:**
  This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
  When there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) decides which of its ports is given the role of the root port by the bridge further away from the root.
  When a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to decide which port it selects locally as the root port. See figure 40 on page 190.
  The root bridge itself does not have a root port.

- **Designated port:**
  The bridge in a network segment that has the lowest root path costs is the designated bridge.
  When more than one bridge has the same root path costs, the bridge with the smallest value bridge identifier becomes the designated bridge. The designated port on this bridge is the port that connects a network segment leading away from the root bridge. When a bridge is connected to a network segment with more than one port (through a hub, for example), the bridge gives the role of the designated port to the port with the better port ID.

- **Edge port:**
  Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).

- **Alternate port:**
  When the connection to the root bridge is lost, this blocked port takes over the task of the root port. The alternate port provides a backup for the connection to the root bridge.
Backup port
This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without any RSTP bridges) is lost.

Disabled port
This is a port that does not participate in the Spanning Tree Operation, that means, the port is switched off or does not have any connection.

Figure 44: Port role assignment

### 12.4.2 Port states

Depending on the tree structure and the state of the selected connection paths, RSTP assigns the ports their states.

Table 32: Relationship between port state values for STP and RSTP

<table>
<thead>
<tr>
<th>STP port state</th>
<th>Administrative bridge port state</th>
<th>MAC Operational</th>
<th>RSTP Port state</th>
<th>Active topology (port role)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>FALSE</td>
<td>Discarding$^1$</td>
<td>Excluded (disabled)</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>FALSE</td>
<td>Discarding$^4$</td>
<td>Excluded (disabled)</td>
</tr>
<tr>
<td>Blocking</td>
<td>Enabled</td>
<td>TRUE</td>
<td>Discarding$^2$</td>
<td>Excluded (alternate, backup)</td>
</tr>
<tr>
<td>Listening</td>
<td>Enabled</td>
<td>TRUE</td>
<td>Discarding$^5$</td>
<td>Included (root, designated)</td>
</tr>
<tr>
<td>Learning</td>
<td>Enabled</td>
<td>TRUE</td>
<td>Learning</td>
<td>Included (root, designated)</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Enabled</td>
<td>TRUE</td>
<td>Forwarding</td>
<td>Included (root, designated)</td>
</tr>
</tbody>
</table>

1. The dot1d-MIB displays Disabled.
2. The dot1d-MIB displays Blocked.

Meaning of the RSTP port states:
- **Disabled**: Port does not belong to the active topology
- **Discarding**: No address learning in FDB, no data traffic except for STP-BPDUs
Learning: Address learning active (FDB), no data traffic apart from STP-BPDUs
Forwarding: Address learning active (FDB), sending and receiving of every packet type (not only STP-BPDUs)

12.4.3 Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RST BPDU and contains the following information:

- Bridge identification of the root bridge
- Root path costs of the sending bridge
- Bridge identification of the sending bridge
- Port identifiers of the ports through which the message was sent
- Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

12.4.4 Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- Introduction of edge-ports:
  During a reconfiguration, RSTP sets an edge port into the transmission mode after 3 seconds (default setting). To ascertain that no bridge sending BPDUs is connected, RSTP waits for the “Hello Time” to elapse.
  When you verify that an end device is and remains connected to this port, there are no waiting times at this port in the case of a reconfiguration.

- Introduction of alternate ports:
  As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternate port after the connection to the root bridge is lost.

- Communication with neighboring bridges (point-to-point connections):
  Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.

- Address table:
  With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.

- Reaction to events:
  Without having to match any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

Note: Data packages could be duplicated and/or arrive at the recipient in the wrong order during the reconfiguration phase of the RSTP topology. You may also use the Spanning Tree Protocol or select another redundancy procedure described in this manual.
12.4.5 Configuring the device

RSTP configures the network topology completely autonomously. The device with the lowest bridge priority automatically becomes the root bridge. However, to define a specific network structure, you specify a device as the root bridge. In general, a device in the backbone takes on this role.

Perform the following steps:

- Set up the network to meet your requirements, initially without redundant lines.
- You deactivate the flow control on the participating ports.
  - If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended. (Default setting: flow control deactivated globally and activated on every port.)
- Disable MRP on every device.
- Enable Spanning Tree on every device in the network.
  - In the state on delivery, Spanning Tree is switched on in the device.

Perform the following steps:

- Open the Switching > L2-Redundancy > Spanning Tree > Global dialog.
- Enable the function.
- Save the settings temporarily. To do this, click the ✓ button.

- In the Priority field you specify a numerically lower value.
  - The bridge with the numerically lowest bridge ID has the highest priority and becomes the root bridge of the network.
- Save the settings temporarily. To do this, click the ✓ button.

After saving, the dialog shows the following information:

- The Bridge is root checkbox is marked.
- The Root port field shows the value 0.0.
- The Root path cost field shows the value 0.
Note: The parameters *Forward delay [s]* and *Max age* have the following relationship:

\[
\text{Forward delay [s]} \geq \frac{(\text{Max age})}{2} + 1
\]

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

Note: When possible, do not change the value in the “Hello Time” field.

Check the following values in the other devices:
- Bridge ID (bridge priority and MAC address) of the corresponding device and the root bridge.
- Number of the device port that leads to the root bridge.
- Path cost from the root port of the device to the root bridge.

Perform the following steps:

1. `show spanning-tree global` To display the parameters for checking.
2. If applicable, then change the values in the *Forward delay [s]* and *Max age* fields.
   - The root bridge transmits the changed values to the other devices.
3. Save the settings temporarily. To do this, click the ✅ button.

- `spanning-tree forward-time <4..30>` To specify the delay time for the status change in seconds.
- `spanning-tree max-age <6..40>` To specify the maximum permissible branch length, for example the number of devices to the root bridge.

- `show spanning-tree global` To display the parameters for checking.
12.4.6 Guards

The device lets you activate various protection functions (guards) in the device ports.

The following protection functions help protect your network from incorrect configurations, loops and attacks with STP-BPDUs:

► BPDU Guard – for manually specified edge ports (end device ports)
  You activate this protection function globally in the device.

Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs on this port, then the device deactivates the device port.

► Root Guard – for designated ports
  You activate this protection function separately for every device port.

When a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to **discarding** instead of **root**.

When there are no STP-BPDUs with better path information to the root bridge, after $2 \times$ **Hello time [s]** the device resets the state of the port to a value according to the port role.
TCN Guard – for ports that receive STP-BPDUs with a Topology Change flag
You activate this protection function separately for every device port.

If the protection function is activated, then the device ignores Topology Change flags in received STP-BPDUs. This does not change the content of the address table (FDB) of the device port. However, additional information in the BPDU that changes the topology is processed by the device.

Loop Guard – for root, alternate and backup ports
You activate this protection function separately for every device port.

If the port does not receive any more STP-BPDUs, then this protection function helps prevent the transmission status of a port from unintentionally being changed to forwarding. If this situation occurs, then the device designates the loop status of the port as inconsistent, but does not forward any data packets.

Activating the BPDU Guard

Perform the following steps:

1. Open the Switching > L2-Redundancy > Spanning Tree > Global dialog.
2. Mark the BPDU guard checkbox.
3. Save the settings temporarily. To do this, click the button.

To change to the Privileged EXEC mode.
When an edge port receives an STP-BPDU, the device behaves as follows:

- The device deactivates this port.
- In the Basic Settings > Port dialog, Configuration tab, the checkbox for this port in the Port on column is unmarked.
- The device designates the port.

You can determine if a port has disabled itself because of a received a BPDU. To do this, perform the following steps:

1. In the Switching > L2-Redundancy > Spanning Tree > Port dialog, Guards tab, the checkbox in the BPDU guard effect column is marked.
2. To display the parameters of the port for checking. The value of the BPDU guard effect parameter is enabled.

Reset the status of the device port to the value forwarding. To do this, perform the following steps:

- When the port still receives BPDUs:
  - Remove the manual definition as an edge port (end device port).
  - Deactivate the BPDU Guard.
- Activate the device port again.
Activating Root Guard / TCN Guard / Loop Guard

Perform the following steps:

- Open the **Switching > L2-Redundancy > Spanning Tree > Port** dialog.
- Switch to the **Guards** tab.
- For designated ports, select the checkbox in the **Root guard** column.
- For ports that receive STP-BPDUs with a Topology Change flag, select the checkbox in the **TCN guard** column.
- For root, alternate or backup ports, mark the checkbox in the **Loop guard** column.

**Note:** The **Root guard** and **Loop guard** functions are mutually exclusive. If you try to activate the **Root guard** function while the **Loop guard** function is active, then the device deactivates the **Loop guard** function.

- Save the settings temporarily. To do this, click the ✔ button.

```
enable
configure
interface <x/y>
spanning-tree guard-root
spanning-tree guard-tcn
spanning-tree guard-loop
exit
show spanning-tree port x/y
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface <x/y>.
To switch the Root Guard on at the designated port.
To switch the TCN Guard on at the port that receives STP-BPDUs with a Topology Change flag.
To switch the Loop Guard on at a root, alternate or backup port.
To display the parameters of the port for checking.
12.5 Link Aggregation

The Link Aggregation function using the single switch method helps you overcome 2 limitations with Ethernet links, namely bandwidth, and redundancy.

The Link Aggregation function helps you overcome bandwidth limitations of individual ports. The Link Aggregation function lets you combine 2 or more links in parallel, creating 1 logical link between 2 devices. The parallel links increase the bandwidth for traffic between the 2 devices.

You typically use the Link Aggregation function on the network backbone. The function provides you an inexpensive way to incrementally increase bandwidth.

Furthermore, the Link Aggregation function provides for redundancy with a seamless failover. When a link goes down, with 2 or more links configured in parallel, the other links in the group continue to forward traffic.

The default settings for a new Link Aggregation instance are as follows:
- In the Active column, the checkbox is marked.
- In the Send trap (Link up/down) column, the checkbox is marked.
- In the Static link aggregation column, the checkbox is unmarked.
- In the Active ports (min.) column, the value is 1.

12.5.1 Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow your network. The single switch method states that you need one device on each side of a link to provide the physical ports. The device balances the traffic load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports are full-duplex, point-to-point links having the same transmission rate. The first port that you add to the group is the master port and determines the bandwidth for the other member ports of the Link Aggregation Group.

The device lets you set up up to 2 Link Aggregation groups. The number of useable ports per Link Aggregation group depends on the device.

12.5.2 Link Aggregation Example

Connect multiple workstations using one aggregated link group between Switch 1 and 2. By aggregating multiple links, higher speeds are achievable without a hardware upgrade.

Figure 45: Link Aggregation Switch to Switch Network
Configure Switch 1 and 2 in the Graphical User Interface. To do this, perform the following steps:

- Open the **Switching > L2-Redundancy > Link Aggregation** dialog.
- Click the **Create** button. The dialog displays the **Create** window.
- From the **Trunk port** drop-down list, select the instance number of the link aggregation group.
- From the **Port** drop-down list, select port 1/1.
- Click the **Ok** button.
- Repeat the preceding steps and select the port 1/2.
- Click the **Ok** button.
- Save the settings temporarily. To do this, click the **✓** button.

```
enable
configure
link-aggregation add lag/1
link-aggregation modify lag/1 addport 1/1
link-aggregation modify lag/1 addport 1/2
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a Link Aggregation Group `lag/1`.
To add port 1/1 to the Link Aggregation Group.
To add port 1/2 to the Link Aggregation Group.
12.6 Link Backup

Link Backup provides a redundant link for traffic on Layer 2 devices. When the device detects an error on the primary link, the device transfers traffic to the backup link. You typically use Link Backup in service-provider or enterprise networks.

You set up the backup links in pairs, one as a primary and one as a backup. When providing redundancy for enterprise networks for example, the device lets you set up more than one pair. The maximum number of link backup pairs is: total number of physical ports / 2. Furthermore, when the state of a port participating in a link backup pair changes, the device sends an SNMP trap.

When configuring link backup pairs, remember the following rules:
- A link pair consists of any combination of physical ports. For example, one port is a 100 Mbit port and the other is a 1000 Mbit SFP port.
- A specific port is a member of one link backup pair at any given time.
- Verify that the ports of a link backup pair are members of the same VLAN with the same VLAN ID. When the primary port or backup port is a member of a VLAN, assign the second port of the pair to the same VLAN.

The default setting for this function is inactive without any link backup pairs.

Note: Verify that the Spanning Tree Protocol is disabled on the Link Backup ports.

12.6.1 Fail Back Description

Link Backup also lets you set up a Fail Back option. When you activate the fail back function and the primary link returns to normal operation, the device first blocks traffic on the backup port and then forwards traffic on the primary port. This process helps protect the device from causing loops in the network.

When the primary port returns to the link up and active state, the device supports 2 modes of operation:
- When you inactivate Fail back, the primary port remains in the blocking state until the backup link fails.
- When you activate Fail back, and after the Fail back delay [s] timer expires, the primary port returns to the forwarding state and the backup port changes to down.

In the cases listed above, the port forcing its link to forward traffic, first sends a topology change packet to the remote device. The topology change packet helps the remote device quickly relearn the MAC addresses.

12.6.2 Example Configuration

In the example network below, you connect ports 2/3 and 2/4 on Switch A to the uplink Switches B and C. When you set up the ports as a Link Backup pair, one of the ports forwards traffic and the other port is in the blocking state.

The primary, port 2/3 on Switch A, is the active port and is forwarding traffic to port 1 on Switch B. Port 2/4 on Switch A is the backup port and blocks traffic.

When Switch A disables port 2/3 because of a detected error, port 2/4 on Switch A starts forwarding traffic to port 2 on Switch C.
When port 2/3 returns to the active state, "no shutdown", with Fail back activated, and Fail back delay [s] set to 30 seconds. After the timer expires, port 2/4 first blocks the traffic and then port 2/3 starts forwarding the traffic.

![Link Backup example network](image)

**Figure 46:** Link Backup example network

The following tables contain examples of parameters to configure Switch A.

Perform the following steps:

1. Open the Switching > L2-Redundancy > Link Backup dialog.
2. Enter a new Link Backup pair in the table:
   - Click the button.
   - The dialog displays the Create window.
   - From the Primary port drop-down list, select port 2/3.
   - From the Backup port drop-down list, select port 2/4.
   - Click the Ok button.
3. In the Description textbox, enter Link_Backup_1 as the name for the backup pair.
4. To activate the Fail back function for the link backup pair, mark the Fail back checkbox.
5. Set the fail back timer for the link backup pair, enter 30 s in Fail back delay [s].
6. To activate the link backup pair, mark the Active checkbox.
7. To enable the function, select the On radio button in the Operation frame.

```
enable
cfg
int 2/3
link-backup add 2/4
link-backup modify 2/4 description Link_Backup_1
link-backup modify 2/4 failback-status enable
link-backup modify 2/4 failback-time 30
link-backup modify 2/4 status enable
exit
link-backup operation
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 2/3.
To create a Link Backup instance where port 2/3 is the primary port and port 2/4 is the backup port.
To specify the string Link_Backup_1 as the name of the backup pair.
To enable the fail back timer.
To specify the fail back delay time as 30 s.
To enable the Link Backup instance.
To change to the Configuration mode.
To enable the Link Backup function globally in the device.
The **FuseNet** protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- RSTP

**Note:** The prerequisite for coupling a network to the main ring using the *Ring/Network Coupling* protocol is that the connected network contains only network devices that support the *Ring/Network Coupling* protocol.

Use the following table to select the **FuseNet** coupling protocol to be used in your network:

<table>
<thead>
<tr>
<th>Main Ring</th>
<th>Connected Network</th>
<th>MRP</th>
<th>RSTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRP</td>
<td></td>
<td></td>
<td>Sub Ring&lt;sup&gt;1)&lt;/sup&gt;</td>
</tr>
<tr>
<td>RSTP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>1)</sup> with MRP configured on different VLANs

---

**Note:**

- no suitable coupling protocol
12.8 Sub Ring

The **Sub Ring** function lets you couple a Sub Ring to a main ring that can use various protocols. The Sub Ring protocol provides redundancy for devices by coupling both ends of an otherwise flat network to a main ring.

The prerequisite is that main ring operates with the one of the following redundancy protocols:

- MRP
- RSTP

Setting up Sub Rings has the following advantages:

- Through the coupling process, you include the new network segment in the redundancy concept.
- Sub Rings allow easy integration of new areas into existing networks.
- Sub Rings allow you easy mapping of the organizational structure of an area in a network topology.
- In a Sub Ring coupled to an MRP Ring, the failover times of the Sub Ring in redundancy cases are typically <100 ms.

12.8.1 Sub Ring description

The Sub Ring concept lets you couple new network segments to suitable devices in an existing ring (main ring). The devices with which you couple the Sub Ring to the main ring are Sub Ring Managers (SRM).

![Diagram of Sub Ring structure](image)

**Figure 47:** Example of a Sub Ring structure
- blue ring = Main ring
- orange ring = Sub Ring
- SRM = Sub Ring Manager
- RM = Ring Manager

The Sub Ring Manager capable devices support up to 8 instances and thus manage up to 8 Sub Rings at the same time.

The **Sub Ring** function lets you integrate devices that support MRP as participants. The devices with which you couple the Sub Ring to the main ring require the **Sub Ring** Manager function.

Each Sub Ring can consist of up to 200 participants, excluding the Sub Ring Managers themselves and the devices between the Sub Ring Managers in the main ring.
The following figures display examples of possible Sub Ring topologies:

Figure 48: Example of an overlapping Sub Ring structure

Figure 49: Special case: A Sub Ring Manager manages 2 Sub Rings (2 instances). The Sub Ring Manager is capable of managing up to 8 instances.

Figure 50: Special case: a Sub Ring Manager manages both ends of a Sub Ring on different ports (Single Sub Ring Manager).

Note: In the previous examples, the Sub Ring Managers only couple Sub Rings to existing main rings. The Sub Ring function prohibits cascaded Sub Rings, for example coupling a new Sub Ring to another existing Sub Ring.
If you use MRP for the main ring, then specify the VLAN settings as follows:

- **VLAN X** for the main ring
  - on the ring ports of the main ring participants
  - on the main ring ports of the Sub Ring Manager
- **VLAN Y** for the Sub Ring (another VLAN ID than VLAN X)
  - on the ring ports of the Sub Ring participants
  - on the Sub Ring ports of the Sub Ring Manager

You can use the same VLAN for multiple Sub Rings.

### 12.8.2 Advanced Information

#### Sub Ring Packets

The protocol Sub Ring uses test packets, link-change packets, and topology-change packets (FDB flush packets).

The 2 SRMs connect the Sub Ring with one Sub Ring port each. The SRMs have different roles, `manager` and `redundantManager`. In case of only one SRM, this SRM has 2 Sub Ring ports. The SRM has the role `singleManager` and takes on the functions of both SRMs in the normal configuration.

As long as the connections in the Sub Ring are operational, the SRM with the role `redundantManager` sets its Sub Ring port into the **blocking** state. In this state, this Sub Ring port receives and sends only Sub Ring packets, it neither receives nor sends normal (payload) data packets. This way, this SRM prevents a network loop in the Sub Ring.

Both SRMs periodically send test packets into the Sub Ring. The test packets are special packets. The SRMs expect to receive the test packets of their partner SRM. The SRM with the role `redundantManager` sends and receives test packets even at its redundant Sub Ring port although the redundant Sub Ring port blocks normal (payload) packets.

If the SRM with the role `redundantManager` does not receive test packets for a specified time, the SRM detects a Sub Ring failure. The SRM then unblocks its redundant Sub Ring port. Conversely, if the SRM again receives test packets from its partner SRM, the SRM sets its redundant port into **blocking**.

On reconfiguration of the Sub Ring, the SRM also flushes its Forwarding Database (FDB) and sends topology-change packets to the Sub Ring participants. The topology-change packets prompt the Sub Ring devices to flush their FDB, too. This procedure helps forward the payload packets over the new path more quickly. This procedure applies regardless whether the Sub Ring reconfiguration was caused by a link-down or a link-up.

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Send Mode</th>
<th>Time Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test packet</td>
<td>Periodically</td>
<td>Send interval</td>
<td>40 ms¹</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reception timeout</td>
<td>280 ms²</td>
</tr>
<tr>
<td>Link-down packet³</td>
<td>Event-driven</td>
<td>On link-down of a Sub Ring port</td>
<td>-</td>
</tr>
<tr>
<td>Topology-change packet⁴</td>
<td>Event-driven</td>
<td>On Sub Ring reconfiguration</td>
<td>-</td>
</tr>
</tbody>
</table>

1. For Sub Ring recovery time 100 ms.
2. The maximum Sub Ring recovery time is 300 ms.
3. Sent by supporting Sub Ring participants.
4. The reception of a topology-change packet prompts the supporting Sub Ring devices to flush their FDB.

### Sub Ring Packet Prioritization

The Sub Ring devices send the test packets, the link-change packets, and the topology-change packets with a user-configurable VLAN ID. The default VLAN ID is 0. The devices send the test packets untagged and thus without priority (Class of Service) information.

To help minimize the reconfiguration time under high network load, you can add a VLAN tag and thus priority information to these packets. The devices then send and forward these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize the test packets, perform the following steps on every device in the Sub Ring:
- Specify the VLAN ID for the Sub Ring test packets to a value \( \geq 1 \).
- Specify the Sub Ring ports as tagged members of this VLAN.

**Note:** When you set the VLAN ID for the Sub Ring packets to a value \( \geq 1 \) in the **Switching > L2-Redundancy > FuseNet > Sub Ring** dialog, the device adds its Sub Ring ports as tagged members of this VLAN. If the VLAN does not yet exist, the device automatically creates this VLAN. After setting a new VLAN ID for the Sub Ring packets, check the **Switching > VLAN > Configuration** dialog for the VLAN and the Sub Ring port membership settings.

### 12.8.3 Sub Ring example

In the following example, you couple a new network segment with 3 devices to an existing main ring which uses the MRP protocol. When you couple the network at both ends instead of one end, the Sub Ring provides increased availability with the corresponding configuration.

You couple the new network segment as a Sub Ring. You couple the Sub Ring to the existing devices of the main ring using the following configuration types.

**Figure 51:** Example of a Sub Ring structure with VLANs
- orange line = Main ring members in VLAN 1
- black line = Sub Ring members in VLAN 2
- orange dashed line = Main ring loop open
- black dashed line = Sub Ring loop open
- SRM = Sub Ring Manager
- RM = Ring Manager
To configure the Sub Ring, perform the following steps:

- Configure the 3 devices of the new network segment as participants in an MRP Ring.
- To minimize the ring recovery time in case of a link-up after a failure, configure the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually configure 100 Mbit/s Full Duplex (FDX).
  - For the other port types, keep the port-specific default settings.

The following steps contain additional settings for Sub Ring configuration:

- To help prevent loops during configuration, deactivate the Sub Ring Manager function on the main ring and Sub Ring devices. After you completely configure every device participating in the main ring and Sub Rings activate the global Sub Ring function and Sub Ring Managers.
- Disable the RSTP function on the MRP Ring ports used in the Sub Ring.
- Verify that the Link Aggregation function is inactive on ports participating in the main ring and Sub Ring.
- To minimize the ring recovery time in case of a link-up after a failure, configure the speed and duplex mode of the Sub Ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually configure 100 Mbit/s Full Duplex (FDX).
  - For the other port types, keep the port-specific default settings.
- Specify a different VLAN membership for the main ring ports and Sub Ring ports although the main ring is using the MRP protocol. For example, use VLAN ID 1 for the main ring and the redundant link, then use VLAN ID 2 for the Sub Ring.
  - For the devices participating in the main ring for example, open the Switching > VLAN > Configuration dialog. Create VLAN 1 in the static VLAN table. To tag the main ring ports for membership in VLAN 1, select the T item from the drop-down list of the appropriate port columns.
  - For the devices participating in the Sub Ring use the step above and add the ports to VLAN 2 in the static VLAN table.
- Activate the MRP function for the main ring and Sub Ring devices.
  - In the Switching > L2-Redundancy > MRP dialog, configure the 2 ring ports participating in the main ring on the main ring devices.
  - For the devices participating in the Sub Ring use the step above and configure the 2 ring ports participating in the Sub Ring on the Sub Ring devices.
  - Assign the same MRP domain ID to the main ring and Sub Ring devices. When you only use Hirschmann devices, the default values suffice for the MRP domain ID.

Note: The MRP domain is a sequence of 16 numbers in the range from 0 to 255. The default value is 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255. An MRP domain ID consisting entirely of zeros is invalid.

The Switching > L2-Redundancy > FuseNet > Sub Ring dialog lets you change the MRP domain ID. Alternatively, use the Command Line Interface. To do this, perform the following steps:

```
enable
configure
mrp domain delete
mrp domain add domain-id 0.0.1.1.2.3.4.111.222.123.0.0.66.99
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To delete the current MRP domain.
To create a new MRP domain with the specified MRP domain ID. Any subsequent MRP domain changes apply to this domain ID.
**12.8.4 Sub Ring example configuration**

**Note:** Help avoid loops during configuration. Configure every device of the Sub Ring individually. Before you activate the redundant link, completely configure every Sub Ring device.

Configure the 2 Sub Ring Managers in the example. To do this, perform the following steps:

- Open the **Switching > L2-Redundancy > FuseNet > Sub Ring** dialog.
- To add a table row, click the button.
- In the **Port** column, select the port that couples the device to the Sub Ring. Use port 1/3 for this example. For coupling, use one of the available ports with the exception of the ports which are already connected to the main ring.
- In the **Name** column, assign a name to the Sub Ring. For this example enter Test.
- In the **SRM mode** column, select Sub Ring Manager mode. You thus specify which port for coupling the Sub Ring to the main ring becomes the redundant port of the Sub Ring Manager.
  - The options for the coupling are:
    - **manager**
      When you specify both Sub Ring Managers with the same value, the device with the higher MAC address manages the redundant link.
    - **redundant manager**
      This device manages the redundant link, as long as you have specified the other Sub Ring Manager as a manager. Otherwise the device with the higher MAC address manages the redundant link.
      Specify Sub Ring Manager 1 as manager, in accordance with the figure depicting this example.
- Leave the values in the **VLAN** column and **MRP domain** column unchanged. The default values are correct for the example configuration.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
sub-ring add 1
sub-ring modify 1 port 1/3
sub-ring modify 1 name Test
sub-ring modify 1 mode manager
show sub-ring ring
show sub-ring global
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a new Sub Ring with the Sub Ring ID 1.
To specify port 1/3 as Sub Ring port.
To assign the name Test to the Sub Ring 1.
To assign the manager mode to the Sub Ring 1.
To display the Sub Rings state on this device.
To display the Sub Ring global state on this device.

- Configure the 2nd Sub Ring Manager in the same way.
  Specify Sub Ring Manager 2 as redundant manager, in accordance with the figure depicting this example.
To activate the Sub Ring Manager function, mark the *Active* checkbox in the corresponding table row.

After you have configured both Sub Ring Managers and the devices participating in the Sub Ring, enable the function and close the redundant link.

Save the settings temporarily. To do this, click the ✅ button.

- `enable`
- `configure`
- `sub-ring enable 1`
- `sub-ring enable 2`
- `exit`
- `show sub-ring ring <Domain ID>`
- `show sub-ring global`
- `copy config running-config nvm profile Test`

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To activate Sub Ring 1.
To activate Sub Ring 2.
To change to the Privileged EXEC mode.
To display the settings of the selected Sub Rings.
To display global Sub Ring settings.
To save the current settings in the configuration profile named `Test` in non-volatile memory (nvm).
12.9 **Sub Ring with LAG**

When at least two parallel redundant connecting lines exist (known as a trunk) between two devices, and these lines are combined into one logical connection, this is a Link Aggregation (LAG) connection.

The device lets you use the LAG ports as ring ports with the **Sub Ring** protocol.

12.9.1 **Example**

The following example is a simple setup between an MRP Ring and a Sub Ring.

![Figure 52: Sub Ring with Link Aggregation](image)

The following table describes the device roles as seen in the figure above. The table provides information of how you use the ring ports and Sub Ring ports as LAG ports.

**Table 34: Devices, Ports and Roles**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Ring Port</th>
<th>Main Ring Role</th>
<th>Sub Ring Role</th>
<th>Sub Ring Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRC1</td>
<td>1/3, 1/4</td>
<td>MRP client</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SRM1</td>
<td>1/3, 1/4</td>
<td>MRP client</td>
<td>Redundant Manager</td>
<td>lag/1</td>
</tr>
<tr>
<td>SRM2</td>
<td>2/4, 2/5</td>
<td>MRP manager</td>
<td>Manager</td>
<td>lag/1</td>
</tr>
<tr>
<td>MRC2</td>
<td>lag/1, 1/3</td>
<td>-</td>
<td>MRP client</td>
<td>-</td>
</tr>
<tr>
<td>MRC3</td>
<td>lag/1, 1/3</td>
<td>-</td>
<td>MRP client</td>
<td>-</td>
</tr>
</tbody>
</table>
**MRP Ring configuration**

The devices participating in the Main ring are members of VLAN 300.

Perform the following steps:

**SRM2**

- `enable`
- `configure`
- `mrp domain add default-domain`
- `mrp domain modify port primary 2/4`
- `mrp domain modify port secondary 2/5`
- `mrp domain modify mode manager`
- `mrp domain modify operation enable`
- `mrp domain modify vlan 300`
- `mrp operation`

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a new MRP domain with the ID `default-domain`.
To specify port 2/4 as ring port 1.
To specify port 2/5 as ring port 2.
To specify that the device operates as the Ring manager. Do not activate the Ring manager function on any other device.
To activate the MRP Ring.
To specify the VLAN ID as 300.
To enable the MRP function in the device.

**MRC1, SRM1**

- `enable`
- `configure`
- `mrp domain add default-domain`
- `mrp domain modify port primary 1/3`
- `mrp domain modify port secondary 1/4`
- `mrp domain modify mode client`
- `mrp domain modify operation enable`
- `mrp domain modify vlan 300`
- `mrp operation`

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a new MRP domain with the ID `default-domain`.
To specify port 1/3 as ring port 1.
To specify port 1/4 as ring port 2.
To specify the device role as ring client.
To activate the MRP Ring.
To specify the VLAN ID as 300.
To enable the MRP function in the device.

**Sub Ring configuration**

The devices participating in the attached Sub Ring are members of VLAN 200.

Perform the following steps:

**SRM1**

- `enable`
- `configure`
- `link-aggregation add lag/1`

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To create a Link Aggregation Group `lag/1`.
link-aggregation modify lag/1 addport 1/1
link-aggregation modify lag/1 addport 1/2
link-aggregation modify lag/1 adminmode

to add port 1/1 to the Link Aggregation Group.
to add port 1/2 to the Link Aggregation Group.
to activate the Link Aggregation Group.

enable
configure
sub-ring add 1
sub-ring modify 1 name SRM1
sub-ring modify 1 mode redundant-manager vlan 200 port lag/1

sub-ring enable 1
sub-ring operation

to create a new Sub Ring with the Sub Ring ID 1.
to assign the name SRM1 to the Sub Ring 1.
to assign the device the role of Sub Ring redundant manager in Sub Ring 1. If the Sub Ring is closed, then the device blocks the ring port. VLAN 200 is the set for the VLAN ID of the domain. The lag/1 port is set as a member in VLAN 200.
to activate Sub Ring 1.
to enable the global Sub Ring Manager functionality on this device.

SRM2

enable
configure
link-aggregation add lag/1
link-aggregation modify lag/1 addport 2/7
link-aggregation modify lag/1 addport 2/8
link-aggregation modify lag/1 adminmode

sub-ring modify 1 name SRM2
sub-ring enable 1
sub-ring operation

to change to the Privileged EXEC mode.
to change to the Configuration mode.
to create a Link Aggregation Group lag/1.
to add port 2/7 to the Link Aggregation Group.
to add port 2/8 to the Link Aggregation Group.
to activate the Link Aggregation Group.

enable
configure
sub-ring add 1
sub-ring modify 1 mode manager vlan 200 port lag/1

sub-ring modify 1 name SRM2
sub-ring enable 1
sub-ring operation

to change to the Privileged EXEC mode.
to change to the Configuration mode.
to create a new Sub Ring with the Sub Ring ID 1.
to assign the device the role of Sub Ring manager in Sub Ring 1. VLAN 200 is the set for the VLAN ID of the domain. The lag/1 port is set as a member in VLAN 200.
to assign the name SRM2 to the Sub Ring 1.
to activate Sub Ring 1.
to enable the global Sub Ring Manager functionality on this device.
**Disable STP**

Disable the Spanning Tree function on every port that you specified as an MRP or Sub Ring port. The following example uses port 1/3.

Perform the following steps:

```
enable
configure
interface 1/3
no spanning-tree operation
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/3.
To disable the Spanning Tree function on the port.
13 Operation diagnosis

The device provides you with the following diagnostic tools:
- Sending SNMP traps
- Monitoring the Device Status
- Out-of-Band signaling using the signal contact
- Event counter at port level
- Detecting non-matching duplex modes
- Auto-Disable
- Displaying the SFP status
- Topology discovery
- Detecting IP address conflicts
- Detecting loops
- Help protect against layer 2 network loops
- Reports
- Monitoring data traffic on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during selftest

13.1 Sending SNMP traps

The device immediately reports unusual events which occur during normal operation to the network management station. This is done by messages called SNMP traps that bypass the polling procedure (“polling” means querying the data stations at regular intervals). SNMP traps allow you to react quickly to unusual events.

Examples of such events are:
- Hardware reset
- Changes to the configuration
- Segmentation of a port

The device sends SNMP traps to various hosts to increase the transmission reliability for the messages. The unacknowledged SNMP trap message consists of a packet containing information about an unusual event.

The device sends SNMP traps to those hosts entered in the trap destination table. The device lets you configure the trap destination table with the network management station using SNMP.
### 13.1.1 List of SNMP traps

The following table displays possible SNMP traps sent by the device.

<table>
<thead>
<tr>
<th>Name of the SNMP trap</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticationFailure</td>
<td>When a station attempts to access an agent without authorisation, this trap is sent.</td>
</tr>
<tr>
<td>coldStart</td>
<td>Sent after the system startup.</td>
</tr>
<tr>
<td>hm2DevMonSenseExtNvmRemoval</td>
<td>When the external memory has been removed, this trap is sent.</td>
</tr>
<tr>
<td>linkDown</td>
<td>When the connection to a port is interrupted, this trap is sent.</td>
</tr>
<tr>
<td>linkUp</td>
<td>When connection is established to a port, this trap is sent.</td>
</tr>
<tr>
<td>hm2DevMonSensePSState</td>
<td>When the status of a power supply unit changes, this trap is sent.</td>
</tr>
<tr>
<td>hm2SigConStateChange</td>
<td>When the status of the signal contact changes in the operation monitoring, this trap is sent.</td>
</tr>
<tr>
<td>newRoot</td>
<td>When the sending agent becomes the new root of the spanning tree, this trap is sent.</td>
</tr>
<tr>
<td>topologyChange</td>
<td>When the port changes from blocking to forwarding or from forwarding to blocking, this trap is sent.</td>
</tr>
</tbody>
</table>
| alarmRisingThreshold                          | When the RMON input exceeds its upper threshold, this trap is sent.  

  *alarmFallingThreshold*  

  When the RMON input goes below its lower threshold, this trap is sent.  

  *hm2AgentPortSecurityViolation*  

  When a MAC address detected on this port does not match the current settings of the parameter *hm2AgentPortSecurityEntry*, this trap is sent.  

  *hm2DiagSelftestActionTrap*  

  When a self test for the four categories “task”, “resource”, “software”, and “hardware” is performed according to the configured settings, this trap is sent.  

  *hm2MrpReconfig*  

  When the configuration of the MRP Ring changes, this trap is sent.  

  *hm2DiagIfaceUtilizationTrap*  

  When the threshold of the interface exceeds or undercut the upper or lower threshold specified, this trap is sent.  

  *hm2LogAuditStartNextSector*  

  When the audit trail after completing one sector starts a new one, this trap is sent.  

  *hm2ConfigurationSavedTrap*  

  After the device has successfully saved its configuration locally, this trap is sent.  

  *hm2ConfigurationChangedTrap*  

  When you change the configuration of the device for the first time after it has been saved locally, this trap is sent.  

  *hm2PlatformStpInstanceLoopInconsistentStartTrap*  

  When the port in this STP instance changes to the “loop inconsistent” status, this trap is sent.  

  *hm2PlatformStpInstanceLoopInconsistentEndTrap*  

  When the port in this STP instance leaves the “loop inconsistent” status receiving a BPDU packet, this trap is sent.
13.1.2 SNMP traps for configuration activity

After you save a configuration in the memory, the device sends a `hm2ConfigurationSavedTrap`. This SNMP trap contains both the state variables of non-volatile memory (NVM) and external memory (ENVM) indicating if the running configuration is in sync with the non-volatile memory, and with the external memory. You can also trigger this SNMP trap by copying a configuration file to the device, replacing the active saved configuration.

Furthermore, the device sends a `hm2ConfigurationChangedTrap`, whenever you change the local configuration, indicating a mismatch between the running and saved configuration.

13.1.3 SNMP trap setting

The device lets you send an SNMP trap as a reaction to specific events. Create at least one trap destination that receives SNMP traps.

Perform the following steps:

- Open the Diagnostics > Status Configuration > Alarms (Traps) dialog.
- Click the + button. The dialog displays the Create window.
- In the Name frame, specify the name that the device uses to identify itself as the source of the SNMP trap.
- In the Address frame, specify the IP address of the trap destination to which the device sends the SNMP traps.
- In the Active column, select the entries that the device takes into account when it sends SNMP traps.
- Save the settings temporarily. To do this, click the ✓ button.

For example, in the following dialogs you specify when the device triggers an SNMP trap:

- Basic Settings > Port dialog
- Basic Settings > Power over Ethernet > Global dialog
- Network Security > Port Security dialog
- Switching > L2-Redundancy > Link Aggregation dialog
- Diagnostics > Status Configuration > Device Status dialog
- Diagnostics > Status Configuration > Security Status dialog
- Diagnostics > Status Configuration > Signal Contact dialog
- Diagnostics > Status Configuration > MAC Notification dialog
- Diagnostics > System > IP Address Conflict Detection dialog
- Diagnostics > System > Selftest dialog
- Diagnostics > Ports > Port Monitor dialog
13.1.4 ICMP messaging

The device lets you use the Internet Control Message Protocol (ICMP) for diagnostic applications, for example ping and trace route. The device also uses ICMP for time-to-live and discarding messages in which the device forwards an ICMP message back to the packet source device.

Use the ping network tool to test the path to a particular host across an IP network. The traceroute diagnostic tool displays paths and transit delays of packets across a network.
13.2 Monitoring the Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

The device displays its current status as \textit{error} or \textit{ok} in the Device status frame. The device determines this status from the individual monitoring results.

The device lets you:

\begin{itemize}
\item Out-of-Band signalling using a signal contact
\item signal the changed device status by sending an SNMP trap
\item detect the device status in the Basic Settings > System dialog of the Graphical User Interface
\item query the device status in the Command Line Interface
\end{itemize}

The \textit{Global} tab of the Diagnostics > Status Configuration > Device Status dialog lets you configure the device to send a trap to the management station for the following events:

\begin{itemize}
\item Incorrect supply voltage
  \begin{itemize}
  \item at least one of the 2 supply voltages is not operating
  \item the internal supply voltage is not operating
  \end{itemize}
\item When the device is operating outside of the user-defined temperature threshold values
\item Loss of the redundancy (in ring manager mode)
\item The interruption of link connection(s)
\end{itemize}

Configure at least one port for this feature. When the link is down, you specify which ports the device signals in the Port tab of the Diagnostics > Status Configuration > Device Status dialog in the Propagate connection error column.

\begin{itemize}
\item The removal of the external memory
\item The configuration in the external memory is out-of-sync with the configuration in the device.
\item The removal of a module
\end{itemize}

Select the corresponding entries to decide which events the device status includes.

\textbf{Note}: With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

13.2.1 Events which can be monitored

\begin{table}[h]
\centering
\caption{Device Status events}
\begin{tabular}{|l|l|}
\hline
\textbf{Name} & \textbf{Meaning} \\
\hline
Connection errors & Activate this function to monitor every port link event in which the Propagate connection error checkbox is marked. \\
\hline
Temperature & Activate this function to monitor when the temperature exceeds or falls below the specified threshold values. \\
\hline
Ethernet module removal & Activate this function to monitor the removal of a module. Also activate the individual module to monitor. \\
\hline
External memory removal & Activate this function to monitor the presence of an external storage device. \\
\hline
External memory not in sync & The device monitors synchronization between the device configuration and the configuration stored in the external memory (ENVM). \\
\hline
Ring redundancy & When ring redundancy is present, activate this function to monitor. \\
\hline
Power supply & Activate this function to monitor the power supply. \\
\hline
\end{tabular}
\end{table}
### Configuring the Device Status

Perform the following steps:

- Open the **Diagnostics > Status Configuration > Device Status** dialog, **Global** tab.
- For the parameters to be monitored, mark the checkbox in the **Monitor** column.
- To send an SNMP trap to the management station, activate the **Send trap** function in the **Traps** frame.
- In the **Diagnostics > Status Configuration > Alarms (Traps)** dialog, create at least one trap destination that receives SNMP traps.
- Save the settings temporarily. To do this, click the ✔️ button.
- Open the **Basic Settings > System** dialog.
- To monitor the temperature, in the **System data** frame, you specify the temperature threshold values.
- Save the settings temporarily. To do this, click the ✔️ button.

---

- **enable** To change to the Privileged EXEC mode.
- **configure** To change to the Configuration mode.
- **device-status trap** To send an SNMP trap when the device status changes.
- **device-status monitor envm-not-in-sync** To monitor the configuration profiles in the device and in the external memory. The **Device status** changes to **error** in the following situations:
  - The configuration profile only exists in the device.
  - The configuration profile in the device differs from the configuration profile in the external memory.
- **device-status monitor envm-removal** To monitor the active external memory. When you remove the active external memory from the device, the value in the **Device status** frame changes to **error**.
- **device-status monitor power-supply 1** To monitor the power supply unit 1. When the device has a detected power supply fault, the value in the **Device status** frame changes to **error**.
- **device-status monitor ring-redundancy** To monitor the ring redundancy. The **Device status** changes to **error** in the following situations:
  - The redundancy function becomes active (loss of redundancy reserve).
  - The device is a normal ring participant and detects an error in its settings.
In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- Open the Diagnostics > Status Configuration > Device Status dialog, Global tab.
- For the Connection errors parameter, mark the checkbox in the Monitor column.
- Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.
- For the Propagate connection error parameter, mark the checkbox in the column of the ports to be monitored.
- Save the settings temporarily. To do this, click the ✅ button.

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the value in the Device status frame changes to error.
To change to the interface configuration mode of interface 1/1.
To monitor the port/interface link. When the link interrupts on the port/interface, the value in the Device status frame changes to error.

**Note:** The above commands activate monitoring and trapping for the supported components. When you want to activate or deactivate monitoring for individual components, you will find the corresponding syntax in the “Command Line Interface” reference manual or in the help of the Command Line Interface console. To display the help in Command Line Interface, insert a question mark ? and press the <Enter> key.

### 13.2.3 Displaying the Device Status

Perform the following steps:

- Open the Basic Settings > System dialog.
enable
show device-status all

To change to the Privileged EXEC mode.
To display the device status and the setting for the device status determination.
13.3 Security Status

The Security Status provides an overview of the overall security of the device. Many processes aid in system visualization by recording the security status of the device and then presenting its condition in graphic form. The device displays the overall security status in the Basic Settings > System dialog, Security status frame.

In the Global tab of the Diagnostics > Status Configuration > Security Status dialog the device displays its current status as error or ok in the Security status frame. The device determines this status from the individual monitoring results.

The device lets you:
- Out-of-Band signalling using a signal contact
- signal the changed security status by sending an SNMP trap
- detect the security status in the Basic Settings > System dialog of the Graphical User Interface
- query the security status in the Command Line Interface

13.3.1 Events which can be monitored

Perform the following steps:
- Specify the events that the device monitors.
- For the corresponding parameter, mark the checkbox in the Monitor column.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password default settings unchanged</td>
<td>After installation change the passwords to increase security. When active and the default passwords remain unchanged, the device displays an alarm.</td>
</tr>
<tr>
<td>Min. password length &lt; 8</td>
<td>Create passwords more than 8 characters long to maintain a high security posture. When active, the device monitors the Min. password length setting.</td>
</tr>
<tr>
<td>Password policy settings deactivated</td>
<td>The device monitors the settings located in the Device Security &gt; User Management dialog for password policy requirements.</td>
</tr>
<tr>
<td>User account password policy check deactivated</td>
<td>The device monitors the settings of the Policy check checkbox. When Policy check is inactive, the device sends an SNMP trap.</td>
</tr>
<tr>
<td>Telnet server active</td>
<td>Activate this function to monitor when the Telnet function is active.</td>
</tr>
<tr>
<td>HTTP server active</td>
<td>Activate this function to monitor when the HTTP function is active.</td>
</tr>
<tr>
<td>SNMP unencrypted</td>
<td>Activate this function to monitor when the SNMPv1 or SNMPv2 function is active.</td>
</tr>
<tr>
<td>Access to system monitor with serial interface possible</td>
<td>The device monitors the System Monitor status.</td>
</tr>
<tr>
<td>Saving the configuration profile on the external memory possible</td>
<td>The device monitors the possibility to save configurations to the external non-volatile memory.</td>
</tr>
<tr>
<td>Link interrupted on enabled device ports</td>
<td>The device monitors the link status of active ports.</td>
</tr>
<tr>
<td>Access with HiDiscovery possible</td>
<td>Activate this function to monitor when the HiDiscovery function has write access to the device.</td>
</tr>
</tbody>
</table>
Table 37: Security Status events (cont.)

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load unencrypted config from external memory</td>
<td>The device monitors the security settings for loading the configuration from the external NVM.</td>
</tr>
<tr>
<td>IEC61850-MMS active</td>
<td>The device monitors the IEC 61850-MMS protocol activation setting.</td>
</tr>
<tr>
<td>Self-signed HTTPS certificate present</td>
<td>The device monitors the HTTPS server for self-created digital certificates.</td>
</tr>
<tr>
<td>Modbus TCP active</td>
<td>The device monitors the Modbus TCP/IP protocol activation setting.</td>
</tr>
</tbody>
</table>

13.3.2 Configuring the Security Status

Perform the following steps:

- Open the Diagnostics > Status Configuration > Security Status dialog, Global tab.
- For the parameters to be monitored, mark the checkbox in the Monitor column.
- To send an SNMP trap to the management station, activate the Send trap function in the Traps frame.
- Save the settings temporarily. To do this, click the ✓ button.
- In the Diagnostics > Status Configuration > Alarms (Traps) dialog, create at least one trap destination that receives SNMP traps.

- `enable` To change to the Privileged EXEC mode.
- `configure` To change to the Configuration mode.
- `security-status monitor pwd-change` To monitor the password for the locally set up user account `admin`. When the password for the `admin` user account is the default setting, the value in the Security status frame changes to `error`.
- `security-status monitor pwd-min-length` To monitor the value specified in the Min. password length policy. When the value for the Min. password length policy is less than 8, the value in the Security status frame changes to `error`.
- `security-status monitor pwd-policy-config` To monitor the password policy settings. When the value for at least one of the following policies is specified as 0, the value in the Security status frame changes to `error`.
  - Upper-case characters (min.)
  - Lower-case characters (min.)
  - Digits (min.)
  - Special characters (min.)
- `security-status monitor pwd-policy-inactive` To monitor the password policy settings. When the value for at least one of the following policies is specified as 0, the value in the Security status frame changes to `error`.
- `security-status monitor telnet-enabled` To monitor the Telnet server. When you enable the Telnet server, the value in the Security status frame changes to `error`. 
In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- Open the Diagnostics > Status Configuration > Security Status dialog, Global tab.
- For the Link interrupted on enabled device ports parameter, mark the checkbox in the Monitor column.
- Save the settings temporarily. To do this, click the ✅ button.
- Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.
- For the Link interrupted on enabled device ports parameter, mark the checkbox in the column of the ports to be monitored.
- Save the settings temporarily. To do this, click the ✅ button.

(enable)

To change to the Privileged EXEC mode.

(configure)

To change to the Configuration mode.

security-status monitor no-link-enabled

To monitor the link on active ports. When the link interrupts on an active port, the value in the Security status frame changes to error.

(interface 1/1)

To change to the interface configuration mode of interface 1/1.

security-status monitor no-link

To monitor the link on interface/port 1.
13.3.3 Displaying the Security Status

Perform the following steps:

- Open the Basic Settings > System dialog.

  - enable
  - show security-status all

To change to the Privileged EXEC mode.

To display the security status and the setting for the security status determination.
13.4 Out-of-Band signaling

The device uses the signal contact to control external devices and monitor device functions. Function monitoring lets you perform remote diagnostics.

The device reports the operating status using a break in the potential-free signal contact (relay contact, closed circuit) for the selected mode. The device monitors the following functions:

- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When the device is operating outside of the user-defined temperature threshold values
- Events for ring redundancy
  Loss of the redundancy (in ring manager mode)
  In the default setting, ring redundancy monitoring is inactive. The device is a normal ring participant and detects an error in the local configuration.
- The interruption of link connection(s)
  Configure at least one port for this feature. In the Propagate connection error frame, you specify which ports the device signals for a link interruption. In the default setting, link monitoring is inactive.
- The removal of the external memory.
- The configuration in the external memory does not match the configuration in the device.
- The removal of a module

Select the corresponding entries to decide which events the device status includes.

**Note:** With a non-redundant voltage supply, the device reports the absence of a supply voltage. To disable this message, feed the supply voltage over both inputs or ignore the monitoring.

13.4.1 Controlling the Signal contact

With the Manual setting mode you control this signal contact remotely.

Application options:

- Simulation of an error detected during SPS error monitoring
- Remote control of a device using SNMP, such as switching on a camera

Perform the following steps:

- Open the Diagnostics > Status Configuration > Signal Contact dialog, Global tab.
- To control the signal contact manually, in the Configuration frame, select the Manual setting item from the Mode drop-down list.
- To open the signal contact, you select the open radio button in the Configuration frame.
- To close the signal contact, you select the close radio button in the Configuration frame.
- Save the settings temporarily. To do this, click the ✅ button.

**enable configure**

To change to the Privileged EXEC mode.

To change to the Configuration mode.
13.4.2 Monitoring the Device and Security_statuses

In the Configuration field, you specify which events the signal contact indicates.

- **Device status**
  
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status dialog.

- **Security status**
  
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Security Status dialog.

- **Device/Security status**
  
  Using this setting the signal contact indicates the status of the parameters monitored in the Diagnostics > Status Configuration > Device Status and the Diagnostics > Status Configuration > Security Status dialog.

Configuring the operation monitoring

Perform the following steps:

- Open the Diagnostics > Status Configuration > Signal Contact dialog, Global tab.
- To monitor the device functions using the signal contact, in the Configuration frame, specify the value Monitoring correct operation in the Mode field.
- For the parameters to be monitored, mark the checkbox in the Monitor column.
- To send an SNMP trap to the management station, activate the Send trap function in the Traps frame.
- Save the settings temporarily. To do this, click the ✓ button.
- In the Diagnostics > Status Configuration > Alarms (Traps) dialog, create at least one trap destination that receives SNMP traps.
- Save the settings temporarily. To do this, click the ✓ button.
- You specify the temperature threshold values for the temperature monitoring in the Basic Settings > System dialog.

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To monitor the temperature in the device. When the temperature exceeds or falls below the specified threshold values, the signal contact opens.
In order to enable the device to monitor an active link without a connection, first enable the global function, then enable the individual ports.

Perform the following steps:

- In the Monitor column, activate the Link interrupted on enabled device ports function.
- Open the Diagnostics > Status Configuration > Device Status dialog, Port tab.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>signal-contact 1 monitor link-failure</td>
<td>To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.</td>
</tr>
<tr>
<td>interface 1/1</td>
<td>To change to the interface configuration mode of interface 1/1.</td>
</tr>
<tr>
<td>signal-contact 1 link-alarm</td>
<td>To monitor the port/interface link. When the link interrupts on the port/interface, the signal contact opens.</td>
</tr>
</tbody>
</table>
Events which can be monitored

Table 38: Device Status events

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection errors</td>
<td>Activate this function to monitor every port link event in which the Propagate connection error checkbox is marked.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Activate this function to monitor when the temperature exceeds or falls below the specified threshold values.</td>
</tr>
<tr>
<td>Ethernet module removal</td>
<td>Activate this function to monitor the removal of a module. Also activate the individual module to monitor.</td>
</tr>
<tr>
<td>External memory removed</td>
<td>Activate this function to monitor the presence of an external storage device.</td>
</tr>
<tr>
<td>External memory not in sync with NVM</td>
<td>The device monitors synchronization between the device configuration and the configuration stored in the external memory (ENVM).</td>
</tr>
<tr>
<td>Ring redundancy</td>
<td>When ring redundancy is present, activate this function to monitor.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Activate this function to monitor the power supply.</td>
</tr>
</tbody>
</table>

Displaying the signal contact status

The device gives you additional options for displaying the status of the signal contact:
- Display in the Graphical User Interface
- Query in the Command Line Interface

Perform the following steps:

- Open the Basic Settings > System dialog. The Signal contact status frame displays the signal contact status and informs you about alarms that have occurred.

  ```
  show signal-contact 1 all
  ```

  To display the signal contact settings for the specified signal contact.
13.5 Port event counter

The port statistics table lets experienced network administrators identify possible detected problems in the network.

This table displays the contents of various event counters. The packet counters add up the events sent and the events received. In the Basic Settings > Restart dialog, you can reset the event counters.

Table 39: Examples indicating known weaknesses

<table>
<thead>
<tr>
<th>Counter</th>
<th>Indication of known possible weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received fragments</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Electromagnetic interference in the transmission medium</td>
</tr>
<tr>
<td>CRC Error</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Electromagnetic interference in the transmission medium</td>
</tr>
<tr>
<td></td>
<td>• Inoperable component in the network</td>
</tr>
<tr>
<td>Collisions</td>
<td>• Non-functioning controller of the connected device</td>
</tr>
<tr>
<td></td>
<td>• Network over extended/lines too long</td>
</tr>
<tr>
<td></td>
<td>• Collision or a detected fault with a data packet</td>
</tr>
</tbody>
</table>

Perform the following steps:

- To display the event counter, open the Basic Settings > Port dialog, Statistics tab.
- To reset the counters, in the Basic Settings > Restart dialog, click the Clear port statistics button.

13.5.1 Detecting non-matching duplex modes

Problems occur when 2 ports directly connected to each other have mismatching duplex modes. These problems are difficult to track down. The automatic detection and reporting of this situation has the benefit of recognizing mismatching duplex modes before problems occur.

This situation arises from an incorrect configuration, for example, deactivation of the automatic configuration on the remote port.

A typical effect of this non-matching is that at a low data rate, the connection seems to be functioning, but at a higher bi-directional traffic level the local device records a lot of detected CRC errors, and the connection falls significantly below its nominal capacity.

The device lets you detect this situation and report it to the network management station. In the process, the device evaluates the detected error counters of the port in the context of the port settings.

Possible causes of port error events

The following table lists the duplex operating modes for TX ports, with the possible fault events. The meanings of terms used in the table are as follows:

- **Collisions**
  - In half-duplex mode, collisions mean normal operation.
- Duplex problem
  Mismatching duplex modes.
- EMI
  Electromagnetic interference.
- Network extension
  The network extension is too great, or too many cascading hubs.
- Collisions, Late Collisions
  In full-duplex mode, no incrementation of the port counters for collisions or Late Collisions.
- CRC Error
  The device evaluates these detected errors as non-matching duplex modes in the manual full duplex mode.

Table 40: Evaluation of non-matching of the duplex mode

<table>
<thead>
<tr>
<th>No.</th>
<th>Automatic configuration</th>
<th>Current duplex mode</th>
<th>Detected error events (≥ 10 after link up)</th>
<th>Duplex modes</th>
<th>Possible causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>marked</td>
<td>Half duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>marked</td>
<td>Half duplex</td>
<td>Collisions</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>marked</td>
<td>Half duplex</td>
<td>Late Collisions</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI, network extension</td>
</tr>
<tr>
<td>4</td>
<td>marked</td>
<td>Half duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>5</td>
<td>marked</td>
<td>Full duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>marked</td>
<td>Full duplex</td>
<td>Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>7</td>
<td>marked</td>
<td>Full duplex</td>
<td>Late Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>8</td>
<td>marked</td>
<td>Full duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>9</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>Collisions</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>Late Collisions</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI, network extension</td>
</tr>
<tr>
<td>12</td>
<td>unmarked</td>
<td>Half duplex</td>
<td>CRC Error</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>13</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>None</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>15</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>Late Collisions</td>
<td>OK</td>
<td>EMI</td>
</tr>
<tr>
<td>16</td>
<td>unmarked</td>
<td>Full duplex</td>
<td>CRC Error</td>
<td>Duplex problem detected</td>
<td>Duplex problem, EMI</td>
</tr>
</tbody>
</table>
13.6 Auto-Disable

The device can disable a port due to several configurable reasons. Each reason causes the port to "shut down". In order to recover the port from the shut down state, you can manually clear the condition which caused the port to shut down or specify a timer to automatically re-enable the port.

If the configuration displays a port as enabled, but the device detects an error or change in the condition, then the software shuts down that port. In other words, the device software disables the port because of a detected error or change in the condition.

If a port is auto-disabled, then the device effectively shuts down the port and the port blocks traffic. The port LED blinks green 3 times per period and identifies the reason for the shutdown. In addition, the device creates a log file entry which lists the causes of the deactivation. When you re-enable the port after a timeout using the Auto-Disable function, the device generates a log entry.

The Auto-Disable function provides a recovery function which automatically enables an auto-disabled port after a user-defined time. When this function enables a port, the device sends an SNMP trap with the port number, but without a value for the Reason parameter.

The Auto-Disable function serves the following purposes:
- It assists the network administrator in port analysis.
- It reduces the possibility that this port causes the network to be instable.

The Auto-Disable function is available for the following functions:
- Link flap (Port Monitor function)
- CRC/Fragments (Port Monitor function)
- Duplex Mismatch detection (Port Monitor function)
- Spanning Tree
- Port Security
- Overload detection (Port Monitor function)
- Link speed/Duplex mode detection (Port Monitor function)

In the following example, you configure the device to disable a port due to detected violations to the thresholds specified the Diagnostics > Ports > Port Monitor dialog, CRC/Fragments tab, and then automatically re-enable a port.

Perform the following steps:

- Open the Diagnostics > Ports > Port Monitor dialog, CRC/Fragments tab.
- Verify that the thresholds specified in the table concur to your preferences for port 1/1.
- Open the Diagnostics > Ports > Port Monitor dialog, Global tab.
- To enable the function, select the On radio button in the Operation frame.
- To allow the device to disable the port due to detected errors, mark the checkbox in the CRC/Fragments on column for port 1/1.
In the Action column you can choose how the device reacts to detected errors. In this example, the device disables port 1/1 for threshold violations and then automatically re-enables the port.

- To allow the device to disable and automatically re-enable the port, select the value auto-disable and configure the Auto-Disable function. The value auto-disable only works in conjunction with the Auto-Disable function.

The device can also disable a port without auto re-enabling.

- To allow the device to disable the port only, select the value disable port.

To manually re-enable a disabled port, select the table row of the port and click the button.

- When you configure the Auto-Disable function, the value disable port also automatically re-enables the port.

Open the Diagnostics > Ports > Port Monitor dialog, Auto-disable tab.

- To allow the device to auto re-enable the port after it was disabled due to detected threshold violations, mark the checkbox in the CRC error column.

Open the Diagnostics > Ports > Port Monitor dialog, Port tab.

Specify the delay time as 120 s in the Reset timer [s] column for the ports you want to enable.

**Note:** The Reset item lets you enable the port before the time specified in the Reset timer [s] column counts down.

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/1.

To specify the CRC-Fragment counter to 2000 parts per million.

To set the measure interval to 15 seconds for CRC-Fragment detection.

To specify the waiting period of 120 seconds, after which the Auto-disable function re-enables the port.

To change to the Configuration mode.

To activate the auto-disable CRC function.

To activate the CRC-Fragments condition to trigger an action.

To activate the Port Monitor function.

When the device disables a port due to threshold violations, the device lets you use the following commands to manually reset the disabled port.

**Perform the following steps:**

```
enable
configure
interface 1/1
port-monitor condition crc-fragments count 2000
port-monitor condition crc-fragments interval 15
auto-disable timer 120
exit
auto-disable reason crc-error
port-monitor condition crc-fragments mode
port-monitor operation
```

```
auto-disable reset
```

To change to the Privileged EXEC mode.

To change to the Configuration mode.

To change to the interface configuration mode of interface 1/1.

To let you enable the port before the Timer counts down.
13.7 Displaying the SFP status

The SFP status display lets you look at the current SFP module connections and their properties. The properties include:

- module type
- serial number of media module
- temperature in °C
- transmission power in mW
- receive power in mW

Perform the following step:

- Open the Diagnostics > Ports > SFP dialog.
13.8 Topology discovery

IEEE 802.1AB defines the Link Layer Discovery Protocol (LLDP). LLDP lets you automatically detect the LAN network topology.

Devices with LLDP active:
- broadcast their connection and management information to neighboring devices on the shared LAN. When the receiving device has its LLDP function active, evaluation of the devices occurs.
- receive connection and management information from neighboring devices on the shared LAN, provided these adjacent devices also have LLDP active.
- build a management information database and object definitions for storing information about adjacent devices with LLDP active.

As the main element, the connection information contains an exact, unique identifier for the connection endpoint: MAC (Service Access Point). This is made up of a device identifier which is unique on the entire network and a unique port identifier for this device.
- Chassis identifier (its MAC address)
- Port identifier (its port-MAC address)
- Description of port
- System name
- System description
- Supported system capabilities
- System capabilities currently active
- Interface ID of the management address
- VLAN-ID of the port
- Auto-negotiation status on the port
- Medium, half/full duplex setting and port speed setting
- Information about the VLANs installed in the device (VLAN-ID and VLAN name, irrespective of whether the port is a VLAN participant).

A network management station can call up this information from devices with activated LLDP. This information lets the network management station map the topology of the network.

Non-LLDP devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP devices therefore discard LLDP packets. If you position a non-LLDP capable device between 2 LLDP capable devices, then the non-LLDP capable device prohibits information exchanges between the 2 LLDP capable devices.

The Management Information Base (MIB) for a device with LLDP capability holds the LLDP information in the lldp MIB and in the private HM2-LLDP-EXT-HM-MIB and HM2-LLDP-MIB.

13.8.1 Displaying the Topology discovery results

Display the topology of the network. To do this, perform the following step:

- Open the Diagnostics > LLDP > Topology Discovery dialog, LLDP tab.

When you use a port to connect several devices, for example through a hub, the table contains a line for each connected device.

Activating Display FDB Entries at the bottom of the table lets you display devices without active LLDP support in the table. In this case, the device also includes information from its FDB (forwarding database).
If you connect the port to devices with the topology discovery function active, then the devices exchange LLDP Data Units (LLDPDU) and the topology table displays these neighboring devices.

When a port connects only devices without an active topology discovery, the table contains a line for this port to represent the connected devices. This line contains the number of connected devices.

The FDB address table contains MAC addresses of devices that the topology table hides for the sake of clarity.

### 13.8.2 LLDP-Med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices. Endpoints include devices such as IP phones, or other Voice over IP (VoIP) devices or servers and network devices such as switches. It specifically provides support for VoIP applications. LLDP-MED provides this support using an additional set of common type-length-value (TLV) advertisement messages, for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.

The device supports the following TLV messages:
- capabilities TLV
  - Lets the LLDP-MED endpoints determine the capabilities that the connected device supports and what capabilities the device has enabled.
- Network policy TLV
  - Lets both network connectivity devices and endpoints advertise VLAN configurations and associated attributes for the specific application on that port. For example, the device notifies a phone of the VLAN number. The phone connects to a switch, obtain its VLAN number, and then starts communicating with the call control.

LLDP-MED provides the following functions:
- Network policy discovery, including VLAN ID, 802.1p priority and DiffServ code point (DSCP)
- Device location and topology discovery based on LAN-level MAC/port information
- Endpoint move detection notification, from network connectivity device to the associated VoIP management application
- Extended device identification for inventory management
- Identification of endpoint network connectivity capabilities, for example, multi-port IP Phone with embedded switch or bridge capability
- Application level interactions with the LLDP protocol elements to provide timely startup of LLDP to support rapid availability of an Emergency Call Service
- Applicability of LLDP-MED to Wireless LAN environments, support for Voice over Wireless LAN
13.9 Detecting loops

Loops in the network cause connection interruptions or data loss. This also applies to temporary loops. The automatic detection and reporting of this situation lets you detect it faster and diagnose it more easily.

An incorrect configuration causes loops, for example, deactivating Spanning Tree.

The device lets you detect the effects typically caused by loops and report this situation automatically to the network management station. You have the option here to specify the magnitude of the loop effects that trigger the device to send a report.

BPDU frames sent from the designated port and received on either a different port of the same device or the same port within a short time, is a typical effect of a loop.

To check if the device has detected a loop, perform the following steps:

- Open the Switching > L2-Redundancy > Spanning Tree > Port dialog, CIST tab.
- Check the value in the Port state and Port role fields. If the Port state field displays the value discarding and the Port role field displays the value backup, then the port is in a loop status.
  or
- Open the Switching > L2-Redundancy > Spanning Tree > Port dialog, Guards tab.
- Check the value in the Loop state column. If the field displays the value true, then the port is in a loop status.
13.10 Help protect against layer 2 network loops

The device helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, a poorly connected cable or an incorrect setting in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:

- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

13.10.1 Application example

The figure displays examples for possible layer 2 loops in a network. The Loop Protection function is enabled in every device.

- **A: Active mode**
  Ports that are intended to connect end devices operate in the active mode. The device evaluates and sends loop detection packets on these ports.

- **P: Passive mode**
  Ports which belong to the redundant rings operate in the passive mode. The device only evaluates loop detection packets on these ports.

- **Loop 1..Loop 4**
  Unintentionally configured layer 2 network loops.

![Figure 53: Examples for unintended layer 2 network loops](image-url)
Assign the Loop Protection settings to the ports

For each active and each passive port, assign the settings of the Loop Protection function.

Perform the following steps:

- Open the Diagnostics > Loop Protection dialog.
- In the Global frame, Transmit interval field, adjust the value, if necessary.
- In the Global frame, Receive threshold field, adjust the value, if necessary.
- In the Mode column, specify the behavior of the Loop Protection function on the port:
  - active for ports that are intended to connect end devices
  - passive for ports which belong to the redundant rings
- In the Action column, specify the value all.
  When the device detects a layer 2 loop on this port, then it sends a trap and disables the port using the Auto-Disable function. If necessary, adjust the value.
- In the Active column, mark the checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

Enable
configure
loop-protection tx-interval 5
loop-protection rx-threshold 1
interface 1/1
loop-protection mode active
loop-protection mode passive
loop-protection action all
loop-protection operation exit

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the transmit interval, if necessary.
To specify the receive threshold, if necessary.
To change to the Interface mode.
Example: port 1/1.
To specify the mode active for ports that are intended to connect end devices.
To specify the mode passive for ports which belong to the redundant rings.
To specify the action that the device performs when it detects a layer 2 network loop on this port.
To activate the Loop Protection function on the port.
To change to the Configuration mode.

Activate the Auto-Disable function

After you assigned the Loop Protection settings to the ports, activate the Auto-Disable function.

Perform the following steps:

- In the Configuration frame, mark the Auto-disable checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

To activate the Auto-Disable function.
Enable the Loop Protection function in the device

When finished, enable the *Loop Protection* function in the device.

Perform the following steps:

- In the *Operation* frame, select the *On* radio button.
- Save the settings temporarily. To do this, click the ✓ button.

To enable the *Loop Protection* function in the device.

### 13.10.2 Recommendations for redundant ports

Depending on the *Loop Protection* settings, the device disables ports using the *Auto-Disable* function when the device detects a layer 2 network loop.

If any redundancy function is active on a port, then do not activate the *active* mode on this port. Otherwise, port shutdowns on redundant network paths can be the result. In the example above these are the ports which belong to the redundant rings.

Verify that a redundant network path is available as backup media. The device changes to the redundant path in case of the outage of the primary path.

The following settings help avoid port shutdowns on redundant network paths:

- Disable the *Loop Protection* function on redundant ports.

  or

- Enable the *passive* mode on redundant ports.

The *Loop Protection* function and the *Spanning Tree* function have an effect on each other. The following steps help avoid unexpected behavior of the device:

- Disable the *Spanning Tree* function on the port on which you want to enable the *Loop Protection* function. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *STP active* column.

- Disable the *Spanning Tree* function on the connected port of each connected device. See the *Switching > L2-Redundancy > Spanning Tree* dialog.
13.11 Using the Email Notification function

The device lets you inform users by email about events that have occurred. Prerequisite is that a mail server is available through the network on which the device transfers the emails.

To set up the device to send emails, perform the steps in the following chapters:
- Specify the sender address
- Specify the triggering events
- Specify the recipients
- Specify the mail server
- Enable/disable the Email Notification function
- Send a test email

13.11.1 Specify the sender address

The sender address is the email address that indicates the device which sent the email. In the device, the default setting is switch@hirschmann.com.

Change the preset value. To do this, perform the following steps:

- Open the Diagnostics > Email Notification > Global dialog.
- In the Sender frame, change the value in the Address field. Add a valid email address.
- Save the settings temporarily. To do this, click the ✔️ button.

<table>
<thead>
<tr>
<th>enable</th>
<th>To change to the Privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>logging email from-addr <a href="mailto:user@doma.in">user@doma.in</a></td>
<td>To change the sender address.</td>
</tr>
</tbody>
</table>

13.11.2 Specify the triggering events

The device differentiates between the following severities:

Table 41: Meaning of the severities for events

<table>
<thead>
<tr>
<th>Severity</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>Device not ready for operation</td>
</tr>
<tr>
<td>alert</td>
<td>Immediate user intervention required</td>
</tr>
<tr>
<td>critical</td>
<td>Critical status</td>
</tr>
<tr>
<td>error</td>
<td>Error status</td>
</tr>
<tr>
<td>warning</td>
<td>Warning</td>
</tr>
<tr>
<td>notice</td>
<td>Significant, normal status</td>
</tr>
<tr>
<td>informational</td>
<td>Informal message</td>
</tr>
<tr>
<td>debug</td>
<td>Debug message</td>
</tr>
</tbody>
</table>
You have the option of specifying the events of which the device informs you. For this, assign the desired minimum severity to the notification levels of the device.

The device informs the recipients as follows:

- **Notification immediate**
  - When an event of the severity assigned or more severe occurs, the device sends an email immediately.

- **Notification periodic**
  - When an event of the severity assigned or more severe occurs, the device logs the event in a buffer.
  - The device sends an email with the log file periodically or if the buffer is full.
  - When an event of a lower severity occurs, the device does not log this event.

Perform the following steps:

- Open the **Diagnostics > Email Notification > Global** dialog.
  - In the **Notification immediate** frame, you specify the settings for emails which the device sends immediately.
    - In the **Severity** field, you specify the minimum severity.
    - In the **Subject** field, you specify the subject of the email.

- In the **Notification periodic** frame, you specify the settings for emails which the device sends periodically.
  - In the **Severity** field, you specify the minimum severity.
  - In the **Subject** field, you specify the subject of the email.

- Save the settings temporarily. To do this, click the ✓ button.

```
 Enable
 configure
 logging email severity immediate <level>
 logging email severity periodic <level>
 logging email subject add <immediate | periodic> TEXT
```

### 13.11.3 Change the send interval

The device lets you specify in which interval it sends emails with the log file. The default setting is 30 minutes.

Perform the following steps:

- Open the **Diagnostics > Email Notification > Global** dialog.
  - In the **Notification periodic** frame, you specify the settings for emails which the device sends periodically.
  - Change the value in the **Sending interval [min]** field to change the interval.

- Save the settings temporarily. To do this, click the ✓ button.
13.11 Using the Email Notification function

13.11.4 Specify the recipients

The device lets you specify up to 10 recipients.

Perform the following steps:

- Open the Diagnostics > Email Notification > Recipients dialog.
- To add a table row, click the button.
- In the Notification type column, specify if the device sends the emails to this recipient immediately or periodically.
- In the Address column, specify the email address of the recipient.
- In the Active column, mark the checkbox.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
logging email duration <30..1440>
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the interval at which the device sends emails with log file.

```
enable
configure
logging email to-addr add <1..10>
addr <user@doma.in> msgtype <immediately | periodically>
```

To specify the recipient with the email address user@doma.in. The device manages the settings in memory 1..10.

13.11.5 Specify the mail server

The device supports encrypted and unencrypted connections to the mail server.

Perform the following steps:

- Open the Diagnostics > Email Notification > Mail Server dialog.
- To add a table row, click the button.
- In the IP address column, specify the IP address or the DNS name of the server.
- In the Encryption column, specify the protocol which encrypts the connection between the device and the mail server.
- When the mail server uses a port other than the well-known port, specify the TCP port in the Destination TCP port column.

When the mail server requests an authentication:

- In the User name and Password columns, specify the account credentials which the device uses to authenticate on the mail server.
13.11.6 Enable/disable the Email Notification function

Perform the following steps:

- Open the Diagnostics > Email Notification > Global dialog.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
logging email mail-server add <1..5>
addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>]
[password <PASSWORD>]
[port <1..65535>]
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To specify the mail server with the IP address IP ADDRESS. The device manages the settings in memory 1..5.

13.11.7 Send a test email

The device lets you check the settings by sending a test email.

Prerequisite:
- The email settings are completely specified.
- The Email Notification function is enabled.

Perform the following steps:

- Open the Diagnostics > Email Notification > Mail Server dialog.
- Click the button.
- The dialog displays the Connection test window.
- From the Recipient drop-down list, select to which recipients the device sends the test email.
- In the Message text field, specify the text of the test email.
- Click the Ok button to send the test email.
enable
configure

logging email test msgtype <urgent|non-urgent> TEXT

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To send an email with the content TEXT to the recipients.

When you do not see any detected error messages and the recipients obtain the email, the device settings are correct.
13.12 Reports

The following lists reports and buttons available for diagnostics:
- System Log file
  The log file is an HTML file in which the device writes device-internal events.
- Audit Trail
  Logs successful commands and user comments. The file also includes SNMP logging.
- Persistent Logging
  When the external memory is present, the device saves log entries in a file in the external memory. These files are available after power down. The maximum size, maximum number of retainable files and the severity of logged events are configurable. After obtaining the user-defined maximum size or maximum number of retainable files, the device archives the entries and starts a new file. The device deletes the oldest file and renames the other files to maintain the configured number of files. To review these files use the Command Line Interface or copy them to an external server for future reference.
- Download support information
  This button lets you download system information as a ZIP archive.

In service situations, these reports provide the technician with the necessary information.

13.12.1 Global settings

Using this dialog you enable or disable where the device sends reports, for example, to a Console, a Syslog Server, or a connection to the Command Line Interface. You also set at which severity level the device writes events into the reports.

Perform the following steps:

- Open the Diagnostics > Report > Global dialog.
- To send a report to the console, specify the desired level in the Console logging frame, Severity field.
- To enable the function, select the On radio button in the Console logging frame.
- Save the settings temporarily. To do this, click the ✓ button.

The device buffers logged events in 2 separate storage areas so that the device keeps log entries for urgent events. Specify the minimum severity for events that the device logs to the buffered storage area with a higher priority.

Perform the following steps:

- To send events to the buffer, specify the desired level in the Buffered logging frame, Severity field.
- Save the settings temporarily. To do this, click the ✓ button.

When you activate the logging of SNMP requests, the device logs the requests as events in the Syslog. The Log SNMP get request function logs user requests for device configuration information. The Log SNMP set request function logs device configuration events. Specify the minimum level for events that the device logs in the Syslog.
Perform the following steps:

- Enable the Log SNMP get request function for the device in order to send SNMP Read requests as events to the Syslog server. To enable the function, select the On radio button in the SNMP logging frame.
- Enable the Log SNMP set request function for the device in order to send SNMP Write requests as events to the Syslog server. To enable the function, select the On radio button in the SNMP logging frame.
- Choose the desired severity level for the get and set requests.
- Save the settings temporarily. To do this, click the ✓ button.

When active, the device logs configuration changes made using the Command Line Interface, to the audit trail. This feature is based on the IEEE 1686 standard for Substation Intelligent Electronic Devices.

Perform the following steps:

- Open the Diagnostics > Report > Global dialog. To enable the function, select the On radio button in the CLI logging frame.
- Save the settings temporarily. To do this, click the ✓ button.

The device lets you save the following system information data in one ZIP file on your PC:
- audittrail.html
- config.xml
- defaultconfig.xml
- script
- runningconfig.xml
- supportinfo.html
- systeminfo.html
- systemlog.html

The device creates the file name of the ZIP archive automatically in the format <IP_address>_<system_name>.zip.

Perform the following steps:

- Click the button. After a while, you can download the ZIP archive.
- Select the directory in which you want to save the support information.
- Click the Ok button.
13.12.2 Syslog

The device lets you send messages about device internal events to one or more Syslog servers (up to 8). Additionally, you also include SNMP requests to the device as events in the Syslog.

**Note:** To display the logged events, open the Diagnostics > Report > Audit Trail dialog or the Diagnostics > Report > System Log dialog.

Perform the following steps:

- Open the Diagnostics > Syslog dialog.
- To add a table row, click the button.
- In the **IP address** column, enter the IP address or **Hostname** of the Syslog server. You can specify a valid IPv4 or IPv6 address for the Syslog server.
- In the **Destination UDP port** column, specify the TCP or UDP port on which the Syslog server expects the log entries.
- In the **Min. severity** column, specify the minimum severity level that an event requires for the device to send a log entry to this Syslog server.
- Mark the checkbox in the **Active** column.
- To enable the function, select the **On** radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the button.

In the **SNMP logging** frame, configure the following settings for read and write SNMP requests:

Perform the following steps:

- Open the Diagnostics > Report > Global dialog.
- Enable the **Log SNMP get request** function for the device in order to send SNMP Read requests as events to the Syslog server. To enable the function, select the **On** radio button in the **SNMP logging** frame.
- Enable the **Log SNMP set request** function for the device in order to send SNMP Write requests as events to the Syslog server. To enable the function, select the **On** radio button in the **SNMP logging** frame.
- Choose the desired severity level for the get and set requests.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
logging host add 1 addr 10.0.1.159 severity 3
logging host add 2 addr 2001::1 severity 4
logging syslog operation
exit
show logging host
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.

To add a recipient in the Syslog servers list. The value 3 specifies the severity level of the event that the device logs. The value 3 means **error**.
To add an IPv6 recipient in the Syslog servers list. The value 4 means **warning**.

To enable the **Syslog** function.
To change to the Privileged EXEC mode.
To display the Syslog host settings.
13.12.3 System Log

The device lets you call up a log file of the system events. The table in the Diagnostics > Report > System Log dialog lists the logged events.

Perform the following steps:

- To update the content of the log, click the button.
- To save the content of the log as an HTML file, click the button.
- To delete the content of the log, click the button.
- To search the content of the log for a key word, use the search function of your web browser.

**Note:** You have the option to also send the logged events to one or more Syslog servers.

13.12.4 Syslog over TLS

The Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.

After initiating a connection with a Syslog server, using a TLS handshake, the device validates the certificate received from the server. For this purpose, you transfer the PEM certificate from a remote server or from the external memory onto the device. Verify that the configured IP address or DNS name of the server matches the information provided in the certificate. You find the information in the Common Name or in the Subject Alternative Name fields of the certificate.
The device sends the TLS encrypted Syslog messages over the TCP port specified in the Destination UDP port column.

**Note:** Specify the IP address or DNS name on the server to match the IP Address or DNS name provided in the server certificate. You find the values entered in the certificate as the Common Name or the Subject Alternative Name.

### Example

The given example describes the configuration of the Syslog function. By following these steps, the device lets you send the TLS encrypted Syslog messages over the TCP port specified in the Destination UDP port column.

The Syslog messages that are sent from a device to a syslog server can pass through unsecured networks. To configure a Syslog server over TLS, transfer the CA certificate onto the device.

**Note:** In order for the changes to take effect after loading a new certificate, restart the Syslog function.

Perform the following steps:

- Open the Diagnostics > Syslog dialog.
- To initiate a connection with the Syslog servers, select the **On** radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the ✓ button.
- The device validates the certificate received. The device also authenticates the server and starts sending Syslog messages.
- Transfer the PEM certificate from the remote server or from the external memory onto the device.

```plaintext
enable
configure
logging host add 1 addr 192.168.3.215
logging host add 2 addr 2001::1
logging host modify 1 port 6512 type systemlog
logging host modify 1 transport tls
logging host modify 1 severity informational
exit
copy syslogcacert evmm
show logging host
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To add index 1 to the Syslog server with IPv4 address 192.168.3.215.
To add index 2 to the Syslog server with IPv6 address 2001::1.
To specify the port number 6512 and logging the events in the system log.
To specify the type of transmission as tls.
To specify the type of event to log into the system log as informational.
To change to the Privileged EXEC mode.
To copy CA certificates from external memory to the device.
To display the Syslog host settings.
13.12.5 Audit Trail

The Diagnostics > Report > Audit Trail dialog contains system information and changes to the device configuration performed through the Command Line Interface and SNMP. In the case of device configuration changes, the dialog displays Who changed What and When.

The Diagnostics > Syslog dialog lets you specify up to 8 Syslog servers to which the device sends Audit Trails.

The following list contains log events:
- changes to configuration parameters
- Commands (except `show` commands) using the Command Line Interface
- Command `logging audit-trail <string>` using the Command Line Interface which logs the comment
- Automatic changes to the System Time
- watchdog events
- locking a user after several unsuccessful login attempts
- User login, either locally or remote, using the Command Line Interface
- Manual, user-initiated, logout
- Timed logout after a user-defined period of inactivity in the Command Line Interface
- file transfer operation including a Firmware Update
- Configuration changes using HiDiscovery
- Automatic configuration or firmware updates using the external memory
- Blocked access to the device management due to invalid login
- rebooting
- opening and closing SNMP over HTTPS tunnels
- Detected power failures
13.13 Network analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff and analyze traffic on a network. A couple of reasons for sniffing traffic on a network is to verify connectivity between hosts, or to analyze the traffic traversing the network.

TCPDump in the device provides the possibility to decode or capture packets received and transmitted by the Management CPU. This function is available using the `debug` command. For further information on the TCPDump function, see the “Command Line Interface” reference manual.
13.14 Monitoring the data traffic

The device lets you forward data packets that pass through the device to a destination port. There you can monitor and evaluate the data packets.

The device provides you with the following options:

- Port Mirroring

13.14.1 Port Mirroring

The Port Mirroring function lets you copy data packets from physical source ports to a physical destination port.

You monitor the data traffic on the source ports in the sending and receiving directions with a management tool connected on the destination port, for example an RMON probe. The function has no affect on the data traffic running on the source ports.

![Diagram showing Switch, PLC, Backbone, and RMON-Probe](image)

*Figure 54: Example*

On the destination port, the device only forwards the data packets copied from the source ports.

Before you switch on the Port Mirroring function, mark the checkbox Allow management to access the device management through the destination port. The device lets users access the device management through the destination port without interrupting the active Port Mirroring session.

**Note:** The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.

The VLAN settings on the destination port remain unchanged. Prerequisite for access to the device management on the destination port is that the destination port is a member of the device management VLAN.
Enabling the Port Mirroring function

Perform the following steps:

- Open the Diagnostics > Ports > Port Mirroring dialog.
- Specify the source ports. Mark the checkbox in the Enabled column for the relevant ports.
- Specify the destination port.
  - In the Destination port frame, select the desired port from the Primary port drop-down list.
  - The drop-down list only displays available ports. Ports that are already specified as source ports are unavailable.
- When needed, specify a second destination port.
  - In the Destination port frame, select the desired port from the Secondary port drop-down list.
  - The prerequisite is that you have already specified the primary destination port.
- In order to access the device management through the destination port:
  - In the Destination port frame, mark the Allow management checkbox.
- Save the settings temporarily. To do this, click the ✓ button.

To deactivate the Port Mirroring function and restore the default settings, click the button.
13.15 Self-test

The device checks its assets during the system startup and occasionally thereafter. The device checks system task availability or termination and the available amount of memory. Furthermore, the device checks for application functionality and any hardware degradation in the chip set.

If the device detects a loss in integrity, then the device responds to the degradation with a user-defined action. The following categories are available for configuration.

- **task**: Action to be taken in case a task is unsuccessful.
- **resource**: Action to be taken due to the lack of resources.
- **software**: Action taken for loss of software integrity; for example, code segment checksum or access violations.
- **hardware**: Action taken due to hardware degradation

Configure each category to produce an action in case the device detects a loss in integrity. The following actions are available for configuration.

- **log only**: This action writes a message to the logging file.
- **send trap**: Sends an SNMP trap to the trap destination.
- **reboot**: If activated, then a detected error in the category will cause the device to reboot.

Perform the following steps:

- Open the *Diagnostics > System > Selftest* dialog.
- In the *Action* column, specify the action to perform for a cause.
- Save the settings temporarily. To do this, click the ✔ button.

```
enable
configure
selftest action task log-only
selftest action resource send-trap
selftest action software send-trap
selftest action hardware reboot
```

Disabling these functions lets you decrease the time required to restart the device after a cold start. You find these options in the *Diagnostics > System > Selftest* dialog, *Configuration* frame.

- **RAM test** checkbox
  Activates/deactivates RAM selftest during a cold start.
Operation diagnosis

13.15 Self-test

- **SysMon1 is available** checkbox
  Activates/deactivates System Monitor 1 during a cold start.

- **Load default config on error** checkbox
  Activates/deactivates the loading of the default device configuration in case no readable configuration is available during the system startup.

The following settings block your access to the device permanently in case the device does not detect any readable configuration profile at system startup.

- The **SysMon1 is available** checkbox is unmarked.
- The **Load default config on error** checkbox is unmarked.

This is the case, for example, when the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

Perform the following steps:

```plaintext
selftest ramtest
no selftest ramtest
selftest system-monitor
no selftest system-monitor
show selftest action

Cause     Action
-----------
task       reboot
resource   reboot
software   reboot
hardware   reboot

show selftest settings

Selftest settings
-----------------
Test RAM on cold start......................enabled
System Monitor 1............................enabled
Boot default configuration on error........enabled
```

To activate RAM selftest on cold start.
To deactivate RAM selftest.
To activate System Monitor 1.
To deactivate System Monitor 1.
To display the actions to be taken in the event of device degradation.

To display the selftest settings.
13.16 Copper cable test

Use this feature to test copper cables attached to an interface for a short or open circuit. The test interrupts traffic flow, when in progress, on this port.

The table displays the state and lengths of each individual pair. The device returns a result with the following meaning:

- normal - indicates that the cable is operating properly
- open - indicates an interruption in the cable
- short circuit - indicates a short circuit in the cable
- untested - indicates an untested cable
- Unknown - cable unplugged
14 Advanced functions of the device

14.1 Using the device as a DHCP server

A DHCP server ("Dynamic Host Configuration Protocol") assigns IP addresses, Gateways, and other networking definitions such as DNS and NTP parameters to clients.

The DHCP operations fall into 4 basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgment. Use the acronym DORA which stands for Discovery, Offer, Request, and Acknowledgement to help remember the phases. The server receives client data on UDP port 67 and forwards data to the client on UDP port 68.

The DHCP server provides an IP address pool or "pool", from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry defines either a specific IP address or an IP address range.

The device lets you activate the DHCP server globally and per interface.

14.1.1 IP Addresses assigned per port or per VLAN

The DHCP server assigns a static IP address or dynamic range of IP addresses to a client connected to a port or a VLAN. The device lets you create entries for either a port or a VLAN. When creating an entry to assign an IP address to a VLAN, the port entry grays out. When creating an entry to assign an IP address to a port, the VLAN entry grays out.

Static allocation means that the DHCP server assigns the same IP address to a specific client. The DHCP server identifies the client using a unique hardware ID. A static address entry contains one IP address, and applies it to a port or VLAN on which the server receives a request from a specific client. For static allocation, create a pool entry for the ports or one specific port, enter the IP address, and leave the Last IP address column empty. Specify a hardware ID with which the DHCP server uniquely identifies the client. This ID is either a MAC address, a client ID, a remote ID, or a circuit ID. When a client contacts the server with the configured hardware ID, the DHCP server allocates the static IP address.

The device also lets you assign a dynamic IP address range to ports or VLANs from which the DHCP server allocates a free IP address from a pool. To add a dynamic pool entry for the ports or VLANs, specify the first and last IP addresses for the IP address range, leaving the MAC address, Client ID, Remote ID, and Circuit ID columns empty. Creating multiple pool entries lets you have IP address ranges that contain gaps.
14.1.2 DHCP server static IP address example

In this example, configure the device to allocate a static IP address to a port. The device recognizes clients with unique hardware identification. The Hardware ID in this case is the client MAC address 00:24:E8:D6:50:51. To do this, perform the following steps:

- Open the Advanced > DHCP Server > Pool dialog.
- To add a table row, click the button.
- In the IP address column, specify the value 192.168.23.42.
- In the Port column, specify the value 1/1.
- In the MAC address column, specify the value 00:24:E8:D6:50:51.
- To assign the IP address to the client infinitely, in the Lease time [s] column, specify the value 4294967295.
- Mark the checkbox in the Active column.
- Open the Advanced > DHCP Server > Global dialog.
- For port 1/1, mark the checkbox in the DHCP server active column.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the button.

```
enable
cfg

dhcp-server pool add 1 static 192.168.23.42

dhcp-server pool modify 1 mode interface 1/1

dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51

dhcp-server pool mode 1

dhcp-server pool modify 1 mode leasetime infinite

dhcp-server operation interface 1/1

dhcp-server operation
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To add a table row with index 1. To add the IP address 192.168.23.42 to the static pool.
To assign the static address in index 1 to interface 1/1.
To assign the IP address in index 1 to the device with the MAC address 00:24:E8:D6:50:51.
To enable the index 1 pool entry.
To allocate the IP address to the client infinitely, modify the table row with index 1.
To enable the DHCP server globally.
To change to the interface configuration mode of interface 1/1.
To activate the DHCP Server server function on this port.
14.1.3 DHCP server dynamic IP address range example

The device lets you create dynamic IP address ranges. Leave the MAC address, Client ID, Remote ID and Circuit ID fields empty. To create dynamic IP address ranges with gaps between the ranges add several entries to the table. To do this, perform the following steps:

- Open the **Advanced > DHCP Server > Pool** dialog.
- To add a table row, click the button.
- In the **IP address** column, specify the value 192.168.23.92. This is the first IP address of the range.
- In the **Last IP address** column, specify the value 192.168.23.142. This is the last IP address of the range.
- In the **Lease time [s]** column, the default setting is 60 days.
- In the **Port** column, specify the value 1/2.
- Mark the checkbox in the **Active** column.
- Open the **Advanced > DHCP Server > Global** dialog.
- For port 1/2, mark the checkbox in the **DHCP server active** column.
- To enable the function, select the On radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142
dhcp-server pool modify 2 leasetime {seconds | infinite}
dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180
dhcp-server pool modify 3 leasetime {seconds | infinite}
dhcp-server pool mode 2
dhcp-server pool mode 3
dhcp-server operation
interface 2/1
dhcp-server operation
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
</tbody>
</table>
| dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142 | To add a dynamic pool with an IP range from 192.168.23.92 to 192.168.23.142.
| dhcp-server pool modify 2 leasetime {seconds | infinite} | To enter the Lease Time in seconds or infinite.                             |
| dhcp-server pool modify 3 leasetime {seconds | infinite} | To enter the Lease Time in seconds or infinite.                             |
| dhcp-server pool mode 2 | To enable the index 2 pool entry.                                            |
| dhcp-server pool mode 3 | To enable the index 3 pool entry.                                            |
| dhcp-server operation    | To enable the DHCP server globally.                                          |
| interface 2/1            | To change to the interface configuration mode of interface 2/1.              |
| dhcp-server operation    | To activate the **DHCP Server** server function on this port.              |
14.2 DHCP L2 Relay

A network administrator uses the DHCP Layer 2 Relay Agent to add DHCP client information. This information is required by Layer 3 Relay Agents and DHCP servers to assign an address and configuration to a client.

When a DHCP client and server are in the same IP subnet, they exchange IP address requests and replies directly. However, having a DHCP server on each subnet is expensive and often impractical. An alternative to having a DHCP server in every subnet is to use the network devices to relay packets between a DHCP client and a DHCP server located in a different subnet.

A Layer 3 Relay Agent is generally a router that has IP interfaces in both the client and server subnets and routes traffic between them. However, in Layer 2 switched networks, there are one or more network devices, switches for example, between the client and the Layer 3 Relay Agent or DHCP server. In this case, this device provides a Layer 2 Relay Agent to add the information that the Layer 3 Relay Agent and DHCP server require to perform their roles in address and configuration assignment.

For the DHCPv6 protocol, a Relay Agent is used to add Relay Agent options to DHCPv6 packets exchanged between a client and a DHCPv6 server. The Lightweight DHCPv6 Relay Agent (LDRA) is described in RFC 6221.

The LDRA processes 2 types of messages:
- The first type of message is the Relay-Forward message which contains unique information about the client.
- The second type of message is the Relay-Reply message which the DHCPv6 server sends to the Relay Agent. The Relay Agent then validates the message to include the information encapsulated in the initial Relay-Forward message and if valid, sends the packet to the client.

The Relay-Forward message contains Interface-ID information, also known as Option 18. This option provides information that identifies the interface on which the client request was sent. The device discards DHCPv6 packets that do not contain Option 18 information.

14.2.1 Circuit and Remote IDs

In an IPv4 environment, before forwarding the request of a client to the DHCP server, the device adds the Circuit ID and the Remote ID to the Option 82 field of the DHCP request packet.
- The Circuit ID stores on which port the device received the request of the client.
- The Remote ID contains the MAC address, the IP address, the system name, or a user-defined character string. Using it, the participating devices identify the Relay Agent that received the request of the client.

The device and other Relay Agents use this information to re-direct the answer from the DHCP Relay Agent to the original client. The DHCP server is able to analyze this data for example to assign the client an IP address from a specific address pool.

Also, the replay packet of the DHCP server contains the Circuit ID and the Remote ID. Before forwarding the answer to the client, the device removes the information from the Option 82 field.
14.2.2 DHCP L2 Relay configuration

The Advanced > DHCP L2 Relay > Configuration dialog lets you activate the function on the active ports and on the VLANs. In the Operation frame, select the On radio button. Then click the ✓ button.

The device forwards DHCPv4 packets with Option 82 information and DHCPv6 packets with Option 18 information on those ports for which the checkbox in the Active column and in the Trusted port column is marked. Typically, these are ports in the network of the DHCP server.

The ports to which the DHCP clients are connected, you activate the DHCP L2 Relay function, but leave the Trusted port checkbox unmarked. On these ports, the device discards DHCPv4 packets with Option 82 information and DHCPv6 packets with Option 18 information.

An example configuration for the DHCPv4 L2 Relay function is shown below. The configuration steps for DHCPv6 L2 Relay function are similar, except for the Circuit ID and Remote ID entries that can only be specified for Option 82.

Perform the following steps on Switch 1:

- Open the Advanced > DHCP L2 Relay > Configuration dialog, Interface tab.
- For port 1/1, specify the settings as follows:
  - Mark the checkbox in the Active column.
- For port 1/2, specify the settings as follows:
  - Mark the checkbox in the Active column.
  - Mark the checkbox in the Trusted port column.
- Open the Advanced > DHCP L2 Relay > Configuration dialog, VLAN ID tab.
- Specify the settings for VLAN 2 as follows:
  - Mark the checkbox in the Active column.
  - Mark the checkbox in the Circuit ID column.
  - To use the IP address of the device as the Remote ID, in the Remote ID type column, specify the value ip.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
Perform the following steps on Switch 2:

- Open the **Advanced > DHCP L2 Relay > Configuration** dialog, **Interface** tab.
- For port **1/1** and **1/2**, specify the settings as follows:
  - Mark the checkbox in the **Active** column.
  - Mark the checkbox in the **Trusted port** column.
- To enable the function, select the **On** radio button in the **Operation** frame.
- Save the settings temporarily. To do this, click the ✅ button.

Verify that VLAN 2 is present. Then perform the following steps on Switch 1:
- Configure VLAN 2, and specify port **1/1** as a member of VLAN 2.

```
able
vlan database
dhcp-l2relay circuit-id 2
dhcp-l2relay remote-id ip 2
dhcp-l2relay mode 2
exit
configure
interface 1/1
dhcp-l2relay mode
exit
interface 1/2
dhcp-l2relay trust
dhcp-l2relay mode
exit
dhcp-l2relay mode
```

Perform the following steps on Switch 2:

```
able
configure
interface 1/1
dhcp-l2relay trust
dhcp-l2relay mode
exit
interface 1/2
dhcp-l2relay trust
```

To change to the Privileged EXEC mode.
To change to the VLAN configuration mode.
To activate the Circuit ID and the DHCP Option 82 on VLAN 2.
To specify the IP address of the device as the Remote ID on VLAN 2.
To activate the **DHCP L2 Relay** function on VLAN 2.
To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/1.
To activate the **DHCP L2 Relay** function on the port.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/2.
To specify the port as **Trusted port**.
To activate the **DHCP L2 Relay** function on the port.
To change to the Configuration mode.
To enable the **DHCP L2 Relay** function in the device.

To change to the Privileged EXEC mode.
To change to the interface configuration mode.
To specify the port as **Trusted port**.
To activate the **DHCP L2 Relay** function.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/2.
To specify the port as **Trusted port**.
To activate the **DHCP L2 Relay** function on the port.
To change to the Configuration mode.
To enable the **DHCP L2 Relay** function in the device.
14.3 Using the device as a DNS client

The DNS client queries DNS servers to resolve host names and IP addresses of network devices. Much like a telephone book, the DNS client converts names of devices into IP addresses. When the DNS client receives a request to resolve a new name, the DNS client first queries its internal static database, then the assigned DNS servers for the information. The DNS client saves the queried information in a cache for future requests.

The device lets you configure the DNS client from the DHCP server using the device management VLAN. The device also lets you assign host names to IP addresses statically.

The DNS client provides the following user functions:
- DNS server list, with space for 4 domain name server IP addresses
- static hostname to IP address mapping, with space for 64 configurable static hosts
- host cache, with space for 128 entries

14.3.1 Configuring a DNS server example

Name the DNS client and configure it to query a DNS server to resolve host names. To do this, perform the following steps:

- Open the Advanced > DNS > Client > Static dialog.
- In the Configuration frame, Configuration source field, specify the value user.
- In the Configuration frame, Domain name field, specify the value device1.
- To add a table row, click the button.
- In the Address column, specify the value 192.168.3.5 as the IPv4 address of the DNS server. You can also specify a valid IPv6 address as the IP address of the DNS server.
- Mark the checkbox in the Active column.
- Open the Advanced > DNS > Client > Global dialog.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the button.

(enable configure
dns client source user
dns client domain-name device1
dns client servers add 1 ip 192.168.3.5
dns client servers add 2 ip 2001::1
dns client adminstate)
Configure the DNS client to map static hosts with IP addresses. To do this, perform the following steps:

- Open the Advanced > DNS > Client > Static Hosts dialog.
- To add a table row, click the button.
- In the Name column, enter the value example.com. This is a name of a device in the network.
- In the IP address column, specify the value 192.168.3.9.
- Mark the checkbox in the Active column.
- Save the settings temporarily. To do this, click the button.

```
enable
configure
dns client host add 1 name example.com
   ip 192.168.3.9

dns client adminstate
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To add example.com as a static host with an IP address of 192.168.3.9.
To enable the Client function globally.
14.4 **GARP**

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and Multicast group membership.

If an attribute for a participant is registered or deregistered according to the GARP function, then the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

14.4.1 **Configuring GMRP**

The GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. The GARP function also lets the devices disseminate the information across the network devices that support extended filtering services.

**Note:** Before you enable the GMRP function, verify that the MMRP function is disabled.

The following example describes the configuration of the GMRP function. The device provides a constrained multicast flooding facility on a selected port. To do this, perform the following steps:

- Open the Switching > GARP > GMRP dialog.
- To provide constrained Multicast Flooding on a port, mark the checkbox in the GMRP active column.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
configure
interface 1/1
garp gmrp operation
exit
garp gmrp operation
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td><code>configure</code></td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td><code>interface 1/1</code></td>
<td>To change to the interface configuration mode of interface 1/1.</td>
</tr>
<tr>
<td><code>garp gmrp operation</code></td>
<td>To enable the GMRP function on the port.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td><code>garp gmrp operation</code></td>
<td>To enable the GMRP function globally.</td>
</tr>
</tbody>
</table>
14.4.2 Configuring GVRP

You use the GVRP function to allow the device to exchange VLAN configuration information with other GVRP devices. Thus reducing unnecessary Broadcast and unknown Unicast traffic. Besides the GVRP function dynamically creates and manages VLANs on devices connected through 802.1Q trunk ports.

The following example describes the configuration of the GVRP function. The device lets you exchange VLAN configuration information with other GVRP devices. To do this, perform the following steps:

- Open the Switching > GARP > GVRP dialog.
- To exchange VLAN configuration information with other GVRP devices, mark checkbox in the GVRP active column for the port.
- Save the settings temporarily. To do this, click the ✓ button.

```
enable
cconfigure
interface 3/1
garp gvrp operation
exit
garp gvrp operation
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 3/1.
To enable the GVRP function on the port.
To change to the Configuration mode.
To enable the GVRP function globally.
14.5 MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP), with the Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP).

To confine traffic to the required areas of a network, the MRP applications distribute attribute values to MRP enabled devices across a LAN. The MRP applications register and de-register Multicast group memberships and VLAN identifiers.

Note: The Multiple Registration Protocol (MRP) requires a loop free network. To help prevent loops in your network, use a network protocol such as the Media Redundancy Protocol, Spanning Tree Protocol, or Rapid Spanning Tree Protocol with MRP.

14.5.1 MRP operation

Each participant contains an applicant component and an MRP Attribute Declaration (MAD) component. The applicant component is responsible for forming the attribute values and their registration and de-registration. The MAD component generates MRP messages for transmission and processes messages received from other participants. The MAD component encodes and transmits the attributes to other participants in MRP Data Units (MRPDU). In the switch, an MRP Attribute Propagation (MAP) component distributes the attributes to participating ports.

A participant exists for each MRP application and each LAN port. For example, a participant application exists on an end device and another application exists on a switch port. The Applicant state machine records the attribute and port for each MRP participant declaration on an end device or switch. Applicant state machine variable changes trigger the transmission of MRPDUs to communicate the declaration or withdrawal.

To establish an MMRP instance, an end device first sends a Join empty (JoinMt) message with the appropriate attributes. The switch then floods the JoinMt to the participating ports and to the neighboring switches. The neighboring switches flood the message to their participating port, and so on, establishing a path for the group traffic.

14.5.2 MRP timers

The default timer settings help prevent unnecessary attribute declarations and withdraws. The timer settings allow the participants to receive and process MRP messages before the Leave or LeaveAll timers expire.

When you reconfigure the timers, maintain the following relationships:
- To allow for re-registration after a Leave or LeaveAll event, although there is a lost message, set the value of the LeaveTime as follows: ≥ (2x JoinTime) + 60 in 1/100 s
- To minimize the volume of rejoining traffic generated following a LeaveAll, specify the value for the LeaveAll timer larger than the LeaveTime.
The following list contains various MRP events that the device transmits:

- **Join** - Controls the interval for the next Join message transmission
- **Leave** - Controls the length of time that a switch waits in the Leave state before changing to the withdraw state
- **LeaveAll** - Controls the frequency with which the switch generates LeaveAll messages

When expired, the Periodic timer initiates a Join request MRP message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdraws.

### 14.5.3 MMRP

When a device receives Broadcast, Multicast or unknown traffic on a port, the device floods the traffic to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (MMRP) lets you control the traffic flooding by distributing an attribute declaration to participants on a LAN. The attribute values that the MAD component encodes and transmits on the LAN in MRP messages are Group service requirement information and 48-bit MAC addresses.

The switch stores the attributes in a filtering database as MAC address registration entries. The forwarding process uses the filtering database entries only to transmit data through those ports necessary to reach Group member LANs.

Switches facilitate the group distribution mechanisms based on the Open Host Group concept, receiving packets on the active ports and forwarding only to ports with group members. This way, any MMRP participants requiring packets transmitted to a particular group or groups, requests membership in the group. MAC service users send packets to a particular group from anywhere on the LAN. A group receives these packets on the LANs attached to registered MMRP participants. MMRP and the MAC Address Registration Entries thus restrict the packets to required segments of a loop-free LAN.

In order to maintain the registration and deregistration state and to receive traffic, a port declares interest periodically. Every device on a LAN with the MMRP function enabled maintains a filtering database and forwards traffic having the group MAC addresses to listed participants.

#### MMRP example

In this example, Host A intends to listen to traffic destined to group G1. Switch A processes the MMRP Join request received from host A and sends the request to both of the neighboring switches. The devices on the LAN now recognize that there is a host interested in receiving traffic destined for group G1. When Host B starts transmitting data destined for group G1, the data flows on the path of registrations and Host A receives it.

![MMRP Network for MAC address Registration](image)
Enable the **MMRP** function on the switches. To do this, perform the following steps:

- Open the **Switching > MRP-IEEE > MMRP** dialog, **Configuration** tab.
- To activate port 1 and port 2 as **MMRP** participants, mark the checkbox in the **MMRP** column for port 1 and port 2 on switch 1.
- To activate port 3 and port 4 as **MMRP** participants, mark the checkbox in the **MMRP** column for port 3 and port 4 on switch 2.
- To activate port 5 and port 6 as **MMRP** participants, mark the checkbox in the **MMRP** column for port 5 and port 6 on switch 3.
- To send periodic events allowing the device to maintain the registration of the MAC address group, enable the **Periodic state machine**. Select the **On** radio button in the **Configuration** frame.
- Save the settings temporarily. To do this, click the ✔️ button.

To enable the **MMRP** ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the **MMRP** functions and ports on switches 2 and 3.

```
enable
configure
interface 1/1
mrp-ieee mmrp operation
interface 1/2
mrp-ieee mmrp operation
exit
mrp-ieee mrp periodic-state-machine
mrp-ieee mmrp operation
```

### 14.5.4 MVRP

The Multiple VLAN Registration Protocol (**MVRP**) is an MRP application that provides dynamic VLAN registration and withdraw services on a LAN.

The **MVRP** function provides a maintenance mechanism for the Dynamic VLAN Registration Entries, and for transmitting the information to other devices. This information lets **MVRP**-aware devices establish and update their VLAN membership information. When members are present on a VLAN, the information indicates through which ports the switch forwards traffic to reach those members.

The main purpose of the **MVRP** function is to allow switches to discover some of the VLAN information that you otherwise manually set up. Discovering this information lets switches overcome the limitations of bandwidth consumption and convergence time in large VLAN networks.
MVRP example

Set up a network comprised of MVRP aware switches (1 - 4) connected in a ring topology with end device groups, A1, A2, B1, and B2 in 2 different VLANs, A and B. With STP enabled on the switches, the ports connecting switch 1 to switch 4 are in the discarding state, helping prevent a loop condition.

In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the forwarding database for the port receiving the frames.

The switch then propagates the request to the other ports, and sends the request to the neighboring LANs and switches. This process continues until the switches have registered the VLANs in the forwarding database of the receive port.

Enable MVRP on the switches. To do this, perform the following steps:

- Open the Switching > MRP-IEEE > MVRP dialog, Configuration tab.
- To activate the ports 1 through 3 as MVRP participants, mark the checkbox in the MVRP column for the ports 1 through 3 on switch 1.
- To activate the ports 2 through 4 as MVRP participants, mark the checkbox in the MVRP column for the ports 2 through 4 on switch 2.
- To activate the ports 3 through 6 as MVRP participants, mark the checkbox in the MVRP column for the ports 3 through 6 on switch 3.
- To activate port 7 and port 8 as MVRP participants, mark the checkbox in the MVRP column for port 7 and port 8 on switch 4.
- To maintain the registration of the VLANs, enable the Periodic state machine. Select the On radio button in the Configuration frame.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
To enable the **MVRP** ports on switch 1, use the following commands. Substituting the appropriate interfaces in the commands, enable the **MVRP** functions and ports on switches 2, 3 and 4.

```
enable
configure
interface 1/1
  mrp-ieee mvrp operation
interface 1/2
  mrp-ieee mvrp operation
exit
  mrp-ieee mvrp periodic-state-machine
  mrp-ieee mvrp operation
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To change to the interface configuration mode of interface 1/1.
To enable the **MVRP** function on the port.
To change to the interface configuration mode of interface 1/2.
To enable the **MVRP** function on the port.
To change to the Configuration mode.
To enable the **Periodic state machine** function globally.
To enable the **MVRP** function globally.
15 Industry Protocols

For a long time, automation communication and office communication were on different paths. The requirements and the communication properties were too different.

Office communication moves large quantities of data with low demands with respect to the transfer time. Automation communication moves small quantities of data with high demands with respect to the transfer time and availability.

While the transmission devices in the office are usually kept in temperature-controlled, relatively clean rooms, the transmission devices used in automation are exposed to wider temperature ranges. Dirty, dusty and damp ambient conditions make additional demands on the quality of the transmission devices.

With the continued development of communication technology, the demands and the communication properties have moved closer together. The high bandwidths now available in Ethernet technology and the protocols they support enable large quantities to be transferred and exact transfer times to be specified.

With the creation of the first optical LAN to be active worldwide, at the University of Stuttgart in 1984, Hirschmann laid the foundation for industry-compatible office communication devices. Thanks to Hirschmann's initiative with the world's first rail hub in the 1990s, Ethernet transmission devices such as switches, routers and firewalls are now available for the toughest automation conditions.

The desire for uniform, continuous communication structures encouraged many manufacturers of automation devices to come together and use standards to aid the progress of communication technology in the automation sector. This is why we now have protocols that let us communicate through Ethernet from the office right down to the field level.

Figure 58: Example of communication.
15.1 **IEC 61850/MMS**

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, for example in the control technology of energy suppliers.

This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file in the device.

### 15.1.1 Switch model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (for example the control room software) uses these objects to monitor and configure the device.

![Bridge model based on Technical Report IEC 61850 90-4](image)

**Figure 59:** Bridge model based on Technical Report IEC 61850 90-4

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LN LLN0</td>
<td>Zero logical node of the Bridge IED: Defines the logical properties of the device.</td>
</tr>
<tr>
<td>LN LPHD</td>
<td>Physical Device logical node of the Bridge IED: Defines the physical properties of the device.</td>
</tr>
<tr>
<td>LN LBRI</td>
<td>Bridge logical node: Represents general settings of the bridge functions of the device.</td>
</tr>
<tr>
<td>LN LCCH</td>
<td>Communication Channel logical node: Defines the logical Communication Channel that consists of one or more physical device ports.</td>
</tr>
</tbody>
</table>
15.1.2 Integration into a Control System

**Preparation of the device**

Perform the following steps:
- □ Check that the device has an IP address assigned.
- □ Open the Advanced > Industrial Protocols > IEC61850-MMS dialog.
- □ To start the MMS server, select in the Operation frame the On radio button, and click ✓ button. Afterwards, an MMS client is able to connect to the device and to read and monitor the objects defined in the bridge model.

---

**Table 42: Classes of the bridge model based on TR IEC61850 90-4 (cont.)**

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LN LCCF</td>
<td><strong>Channel Communication Filtering</strong> logical node:</td>
</tr>
<tr>
<td></td>
<td>Defines the VLAN and Multicast settings for the higher-level Communication</td>
</tr>
<tr>
<td></td>
<td>Channel.</td>
</tr>
<tr>
<td>LN LBSP</td>
<td><strong>Port Spanning Tree Protocol</strong> logical node:</td>
</tr>
<tr>
<td></td>
<td>Defines the Spanning Tree statuses and settings for the respective physical</td>
</tr>
<tr>
<td></td>
<td>device port.</td>
</tr>
<tr>
<td>LN LPLD</td>
<td><strong>Port Layer Discovery</strong> logical node:</td>
</tr>
<tr>
<td></td>
<td>Defines the LLDP statuses and settings for the respective physical device</td>
</tr>
<tr>
<td></td>
<td>port.</td>
</tr>
<tr>
<td>LN LPCP</td>
<td><strong>Physical Communication Port</strong> logical node:</td>
</tr>
<tr>
<td></td>
<td>Represents the respective physical device port.</td>
</tr>
</tbody>
</table>
IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and possible problems in the network.

**NOTICE**

**RISK OF UNAUTHORIZED ACCESS TO THE DEVICE**

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

*Failure to follow these instructions can result in equipment damage.*

- To allow the MMS client to change the settings, mark the **Write access** checkbox, and click the ✓ button.

**Offline configuration**

The device lets you download the ICD file using the Graphical User Interface. This file contains the properties of the device described with SCL and lets you configure the substation without directly connecting to the device.

- Open the **Advanced > Industrial Protocols > IEC61850-MMS** dialog.
- To load the ICD file to your PC, click the  button.

**Monitoring the device**

The IEC61850/MMS server integrated into the device lets you monitor multiple statuses of the device by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device lets you monitor the following statuses:

*Table 43: Statuses of the device that can be monitored with IEC 61850/MMS*

<table>
<thead>
<tr>
<th>Class</th>
<th>RCB object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LN LPHD</td>
<td>TmpAlm</td>
<td>When the temperature measured in the device exceeds or falls below the set temperature thresholds, the status changes.</td>
</tr>
<tr>
<td>PhyHealth</td>
<td></td>
<td>When the status of the LPHD.TmpAlm RCB object changes, the status changes.</td>
</tr>
<tr>
<td>LN LPHD</td>
<td>TmpAlm</td>
<td>When the temperature measured in the device exceeds or falls below the set temperature thresholds, the status changes.</td>
</tr>
<tr>
<td>PwrSupAlm</td>
<td></td>
<td>When one of the redundant power supplies becomes inoperative or starts operating again, the status changes.</td>
</tr>
<tr>
<td>PhyHealth</td>
<td></td>
<td>When the status of the LPHD.PwrSupAlm or LPHD.TmpAlm RCB object changes, the status changes.</td>
</tr>
</tbody>
</table>
### Table 43: Statuses of the device that can be monitored with IEC 61850/MMS (cont.)

<table>
<thead>
<tr>
<th>Class</th>
<th>RCB object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LN LBRI</td>
<td>RstpRoot</td>
<td>When the device takes over or relinquishes the role of the root bridge, the status changes.</td>
</tr>
<tr>
<td></td>
<td>RstpTopoCnt</td>
<td>When the topology changes due to a change of the root bridge, the status changes.</td>
</tr>
<tr>
<td>LN LCCH</td>
<td>ChLiv</td>
<td>When the link status of the physical port changes, the status changes.</td>
</tr>
<tr>
<td>LN LPCP</td>
<td>PhyHealth</td>
<td>When the link status of the physical port changes, the status changes.</td>
</tr>
</tbody>
</table>
15.2 Modbus TCP

Modbus TCP is an application layer messaging protocol providing client/server communication between the client and devices connected in Ethernet TCP/IP networks.

The Modbus TCP function lets you install the device in networks already using Modbus TCP and retrieve information saved in the registers in the device.

15.2.1 Client/Server Modbus TCP/IP Mode

The device supports the client/server model of Modbus TCP/IP. This device operates as a server in this constellation and responds to requests from a client for information saved in the registers.

The client / server model uses four types of messages to exchange data between the client and server:
- Modbus TCP/IP Request, the client creates a request for information and sends it to the server.
- Modbus TCP/IP Indication, the server receives a request as an indication that a client requires information.
- Modbus TCP/IP Response, when the required information is available, the server sends a reply containing the requested information. When the requested information is unavailable, the server sends an Exception Response to notify the client of the error detected during the processing. The Exception Response contains an exception code indicating the reason for the detected error.
- Modbus TCP/IP Confirmation, the client receives a response from the server, containing the requested information.

15.2.2 Supported Functions and Memory Mapping

The device supports functions with the public codes 0x03 (Read HoldingRegisters) and 0x05 (Write Single Coil). The codes let you read the information saved in the registers such as the system information, including the system name, system location, software version, IP address, MAC address. The codes also let you read the port information and port statistics. The 0x05 code lets you reset the port counters individually or globally.

The following list contains definitions for the values entered in the Format column:
- Bitmap: a group of 32-bits, encoded into the Big-endian byte order and saved in 2 registers. Big-endian systems save the most significant byte of a word in the smallest address and save the least significant byte in the largest address.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
Industry Protocols
15.2 Modbus TCP

- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- String: octets, saved in sequence, 2 octets per register.

**Modbus TCP/IP Codes**

The addresses in the following tables allow the client to reset port counters and retrieve specific information from the device registers.

**Table 44: System/Global Information**

<table>
<thead>
<tr>
<th>Address</th>
<th>Qty</th>
<th>Description</th>
<th>Min</th>
<th>Max</th>
<th>Step</th>
<th>Unit</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>128</td>
<td>System Name</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0080</td>
<td>128</td>
<td>System Contact</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0100</td>
<td>128</td>
<td>System Location</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0180</td>
<td>128</td>
<td>Software Version</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0200</td>
<td>32</td>
<td>OrderCode</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0220</td>
<td>16</td>
<td>Serial Number</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>0230</td>
<td>1</td>
<td>IP Address[0]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0231</td>
<td>1</td>
<td>IP Address[1]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0232</td>
<td>1</td>
<td>IP Address[2]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0233</td>
<td>1</td>
<td>IP Address[3]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0234</td>
<td>1</td>
<td>NetMask[0]</td>
<td>0</td>
<td>255</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0235</td>
<td>1</td>
<td>NetMask[1]</td>
<td>0</td>
<td>255</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0236</td>
<td>1</td>
<td>NetMask[2]</td>
<td>0</td>
<td>255</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0237</td>
<td>1</td>
<td>NetMask[3]</td>
<td>0</td>
<td>255</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0238</td>
<td>1</td>
<td>GateWay[0]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0239</td>
<td>1</td>
<td>GateWay[1]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>023A</td>
<td>1</td>
<td>GateWay[2]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>023B</td>
<td>1</td>
<td>GateWay[3]</td>
<td>0</td>
<td>254</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>023C</td>
<td>3</td>
<td>MacAddress</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>String</td>
</tr>
<tr>
<td>023F</td>
<td>1</td>
<td>PowerAlarm1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F2</td>
</tr>
<tr>
<td>0240</td>
<td>1</td>
<td>PowerAlarm2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F2</td>
</tr>
<tr>
<td>0241</td>
<td>1</td>
<td>StpState</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0242</td>
<td>2</td>
<td>Number of Ports</td>
<td>1</td>
<td>64</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0244</td>
<td>1</td>
<td>Reset Counter (all Counter)</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0245</td>
<td>4</td>
<td>Port Present Map</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Bitmap</td>
</tr>
<tr>
<td>0249</td>
<td>4</td>
<td>Port Link Map</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Bitmap</td>
</tr>
<tr>
<td>0250</td>
<td>4</td>
<td>Port Stp State Map</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Bitmap</td>
</tr>
<tr>
<td>0251</td>
<td>4</td>
<td>Port Activity Map</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Bitmap</td>
</tr>
</tbody>
</table>
### Table 45: Port Information

<table>
<thead>
<tr>
<th>Address</th>
<th>Qty</th>
<th>Description</th>
<th>Min</th>
<th>Max</th>
<th>Step</th>
<th>Unit</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0400</td>
<td>1</td>
<td>Port 1 Type</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>-</td>
<td>F4</td>
</tr>
<tr>
<td>0401</td>
<td>1</td>
<td>Port 2 Type</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>-</td>
<td>F4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>043F</td>
<td>1</td>
<td>Port 64 Type</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>-</td>
<td>F4</td>
</tr>
<tr>
<td>0440</td>
<td>1</td>
<td>Port 1 Link Status</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0441</td>
<td>1</td>
<td>Port 2 Link Status</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>047F</td>
<td>1</td>
<td>Port 64 Link Status</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0480</td>
<td>1</td>
<td>Port 1 STP State</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0481</td>
<td>1</td>
<td>Port 2 STP State</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04BF</td>
<td>1</td>
<td>Port 64 STP State</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>04C0</td>
<td>1</td>
<td>Port 1 Activity</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>04C1</td>
<td>1</td>
<td>Port 2 Activity</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04FF</td>
<td>1</td>
<td>Port 64 Activity</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0500</td>
<td>1</td>
<td>Port 1 Counter Reset</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td>0501</td>
<td>1</td>
<td>Port 2 Counter Reset</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>053F</td>
<td>1</td>
<td>Port 64 Counter Reset</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>F1</td>
</tr>
</tbody>
</table>

### Table 46: Port Statistics

<table>
<thead>
<tr>
<th>Address</th>
<th>Qty</th>
<th>Description</th>
<th>Min</th>
<th>Max</th>
<th>Step</th>
<th>Unit</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800</td>
<td>2</td>
<td>Port 1 - Number of bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0802</td>
<td>2</td>
<td>Port 1 - Number of bytes sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0804</td>
<td>2</td>
<td>Port 1 - Number of frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0806</td>
<td>2</td>
<td>Port 1 - Number of frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0808</td>
<td>2</td>
<td>Port 1 - Total bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>080A</td>
<td>2</td>
<td>Port 1 - Total frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>080C</td>
<td>2</td>
<td>Port 1 - Number of broadcast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>080E</td>
<td>2</td>
<td>Port 1 - Number of multicast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0810</td>
<td>2</td>
<td>Port 1 - Number of frames with CRC error</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0812</td>
<td>2</td>
<td>Port 1 - Number of oversized frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0814</td>
<td>2</td>
<td>Port 1 - Number of bad fragments received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0816</td>
<td>2</td>
<td>Port 1 - Number of jabber frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0818</td>
<td>2</td>
<td>Port 1 - Number of collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>081A</td>
<td>2</td>
<td>Port 1 - Number of late collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>081C</td>
<td>2</td>
<td>Port 1 - Number of 64-byte frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>081E</td>
<td>2</td>
<td>Port 1 - Number of 65-127 byte frames</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>0820</td>
<td>2</td>
<td>Port 1 - Number of 128-255 byte frames</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
</tbody>
</table>
### Table 46: Port Statistics (cont.)

<table>
<thead>
<tr>
<th>Address</th>
<th>Qty</th>
<th>Description</th>
<th>Min</th>
<th>Max</th>
<th>Step</th>
<th>Unit</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0822</td>
<td>2</td>
<td>Port1 - Number of 256-511 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0824</td>
<td>2</td>
<td>Port1 - Number of 512-1023 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0826</td>
<td>2</td>
<td>Port1 - Number of 1023-MAX byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0828</td>
<td>2</td>
<td>Port1 - Number of Mac Error Packets</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>082A</td>
<td>2</td>
<td>Port1 - Number of dropped received packets</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>082C</td>
<td>2</td>
<td>Port1 - Number of multicast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0830</td>
<td>2</td>
<td>Port1 - Number of broadcast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0832</td>
<td>2</td>
<td>Port2 - Number of bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0834</td>
<td>2</td>
<td>Port2 - Number of bytes sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0836</td>
<td>2</td>
<td>Port2 - Number of frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0838</td>
<td>2</td>
<td>Port2 - Number of frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>083A</td>
<td>2</td>
<td>Port2 - Total bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>083C</td>
<td>2</td>
<td>Port2 - Total frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>083E</td>
<td>2</td>
<td>Port2 - Number of broadcast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0840</td>
<td>2</td>
<td>Port2 - Number of multicast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0842</td>
<td>2</td>
<td>Port2 - Number of frames with CRC error</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0844</td>
<td>2</td>
<td>Port2 - Number of oversized frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0846</td>
<td>2</td>
<td>Port2 - Number of bad fragments rcvd(&lt;64 bytes)</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0848</td>
<td>2</td>
<td>Port2 - Number of jabber frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>084A</td>
<td>2</td>
<td>Port2 - Number of collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>084C</td>
<td>2</td>
<td>Port2 - Number of late collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>084E</td>
<td>2</td>
<td>Port2 - Number of 64-byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0850</td>
<td>2</td>
<td>Port2 - Number of 65-127 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0852</td>
<td>2</td>
<td>Port2 - Number of 128-255 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0854</td>
<td>2</td>
<td>Port2 - Number of 256-511 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0856</td>
<td>2</td>
<td>Port2 - Number of 512-1023 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0858</td>
<td>2</td>
<td>Port2 - Number of 1023-MAX byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>085A</td>
<td>2</td>
<td>Port2 - Number of Mac Error Packets</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>085C</td>
<td>2</td>
<td>Port2 - Number of dropped received packets</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>085E</td>
<td>2</td>
<td>Port2 - Number of multicast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
<tr>
<td>0860</td>
<td>2</td>
<td>Port2 - Number of broadcast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>F9</td>
<td></td>
</tr>
</tbody>
</table>
Table 46: Port Statistics (cont.)

<table>
<thead>
<tr>
<th>Address</th>
<th>Qty</th>
<th>Description</th>
<th>Min</th>
<th>Max</th>
<th>Step</th>
<th>Unit</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0862</td>
<td>2</td>
<td>Port2 - Number of &lt;64 byte fragments w/ good CRC</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>144E</td>
<td>2</td>
<td>Port64 - Number of bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1450</td>
<td>2</td>
<td>Port64 - Number of bytes sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1452</td>
<td>2</td>
<td>Port64 - Number of frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1454</td>
<td>2</td>
<td>Port64 - Number of frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1456</td>
<td>2</td>
<td>Port64 - Total bytes received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1458</td>
<td>2</td>
<td>Port64 - Total frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>145A</td>
<td>2</td>
<td>Port64 - Number of broadcast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>145C</td>
<td>2</td>
<td>Port64 - Number of multicast frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>145E</td>
<td>2</td>
<td>Port64 - Number of frames with CRC error received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1460</td>
<td>2</td>
<td>Port64 - Number of oversized frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1462</td>
<td>2</td>
<td>Port64 - Number of bad fragments rcvd(&lt;64 bytes) received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1464</td>
<td>2</td>
<td>Port64 - Number of jabber frames received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1466</td>
<td>2</td>
<td>Port64 - Number of collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1468</td>
<td>2</td>
<td>Port64 - Number of late collisions occurred</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>146A</td>
<td>2</td>
<td>Port64 - Number of 64-byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>146C</td>
<td>2</td>
<td>Port64 - Number of 65-127 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>146E</td>
<td>2</td>
<td>Port64 - Number of 128-255 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1470</td>
<td>2</td>
<td>Port64 - Number of 256-511 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1472</td>
<td>2</td>
<td>Port64 - Number of 512-1023 byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1474</td>
<td>2</td>
<td>Port64 - Number of 1023-MAX byte frames rcvd/sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1476</td>
<td>2</td>
<td>Port64 - Number of Mac Error Packets received</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>1478</td>
<td>2</td>
<td>Port64 - Number of dropped received packets sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>147A</td>
<td>2</td>
<td>Port64 - Number of multicast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>147C</td>
<td>2</td>
<td>Port64 - Number of broadcast frames sent</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
<tr>
<td>147E</td>
<td>2</td>
<td>Port64 - Number of &lt;64 byte fragments w/ good CRC</td>
<td>0</td>
<td>4294967295</td>
<td>1</td>
<td>-</td>
<td>F9</td>
</tr>
</tbody>
</table>
15.2.3 Example Configuration

In this example, you configure the device to respond to client requests. The prerequisite for this configuration is that the client device is configured with an IP address within the given range. The Write access function remains inactive for this example. When you activate the Write access function, the device lets you reset the port counters only. In the default setting the Modbus TCP and Write access functions are inactive.

The Modbus TCP protocol does not provide any authentication mechanisms. If the write access for Modbus TCP is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. This in turn can result in an incorrect configuration of the device and possible problems in the network.

**NOTICE**

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

Perform the following steps:

- Open the Device Security > Management Access > IP Access Restriction dialog.
- Add a table row. To do this, click the button.
- Specify the IP address range in the table row where the Index column has the value 2. To do this, enter the following values:
  - In the Address column: 10.17.1.0
  - In the Netmask column: 255.255.255.248
- Verify that the checkbox in the Modbus TCP column is marked.
- Activate the IP address range. To do this, mark the checkbox in the Active column.
- Save the settings temporarily. To do this, click the button.
- Open the Diagnostics > Status Configuration > Security Status dialog, Global tab.
- Verify that the checkbox related to the parameter Modbus TCP active is marked.
- Open the Advanced > Industrial Protocols > Modbus TCP dialog.
- The standard Modbus TCP listening port, port 502, is the default setting. However, when you wish to listen on another TCP port, enter the value for the listening port in the TCP port field.
- To enable the function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the button.

When you enable the Modbus TCP function, the Security Status function detects the activation and displays an alarm in the Basic Settings > System dialog, Security status frame.

### Command Line

```
enable
network management access add 2
network management access modify 2 ip 10.17.1.0
```

To change to the Privileged EXEC mode.

To create the entry for the address range in the network. Number of the next available index in this example: 2.

To specify the IP address.
network management access modify 2 mask 29
network management access modify 2
modbus-tcp enable
network management access operation
configure
security-status monitor modbus-tcp-enabled
modbus-tcp operation
modbus-tcp port <1..65535>

show modbus-tcp
Modbus TCP/IP server settings
-----------------------------
Modbus TCP/IP server operation..............enabled
Write-access..................................disabled
Listening port...............................502
Max number of sessions.....................5
Active sessions..............................0
show security-status monitor
Device Security Settings
Monitor
-----------------------------------
Password default settings unchanged.........monitored
...
Write access using HiDiscovery is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled..................monitored
Modbus TCP/IP server active................monitored
show security-status event
To display occurred security status events.
Time stamp               Event                     Info
------------------------  ------------------------  ------
2014-01-01 01:00:39     password-change(10)       -
2014-01-01 01:00:39     ext-nvm-load-unsecure(21) -
2014-01-01 23:47:40     modbus-tcp-enabled(23)    -
show network management access rules 1
To display the restricted management access rules for index 1.

 Restricted management access settings
--------------------------------------
Index...........................................1
IP Address..................................10.17.1.0
Prefix Length..............................29
HTTP..........................................yes
SNMP.........................................yes
Telnet........................................yes
SSH..........................................yes
HTTPS........................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP..............................yes
Active......................................[x]
15.3 **OPC UA Server**

The *Open Platform Communications United Architecture (OPC UA)* is a protocol for industrial communication, and describes a variety of *OPC UA* information models. The *OPC UA* protocol is a standardized protocol for the secure and reliable exchange of data in the industrial automation space and in other industries.

The *OPC UA* protocol provides a very flexible and adaptable mechanism for transferring the data between industrial automation equipment, monitoring devices, and sensors. The *OPC UA* protocol uses a standard interface, for example, HTTPS that makes the protocol simple to integrate into existing management systems. The device operating as an *OPC UA* server transmits the data of the connected end devices, ranging from simple uptime status to large amounts of complex industrial data.

The following figure displays the *OPC UA* information model data of the connected end devices available to the *OPC UA* client.

![Figure 61: OPC UA information model](image)

*Figure 61: OPC UA information model*
### Table 47: Objects in the OPC UA information model

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto power down</strong></td>
<td>Specifies how the port behaves when no cable is connected.</td>
</tr>
<tr>
<td><strong>Port on</strong></td>
<td>Activates/deactivates the port.</td>
</tr>
<tr>
<td><strong>Power state (port off)</strong></td>
<td>Specifies if the port is physically switched on or off when you deactivate the port with the Port on function.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Displays if the port is currently physically enabled or disabled.</td>
</tr>
<tr>
<td><strong>Port status</strong></td>
<td>Displays the link status of the port.</td>
</tr>
</tbody>
</table>

### Table 48: Object values in the OPC UA information model

<table>
<thead>
<tr>
<th>Object</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Error Reason</strong></td>
<td>1</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Power supply</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Link failure</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Temperature</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Fan failure</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Module removal</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>External non volatile memory removal</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>External non volatile memory not in synchronization</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Ring redundancy</td>
</tr>
<tr>
<td><strong>External Non Volatile Memory 1 Status</strong></td>
<td>1</td>
<td>Not present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Removed</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Out of memory</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Generic error</td>
</tr>
<tr>
<td><strong>External Non Volatile Memory 2 Status</strong></td>
<td>1</td>
<td>Not present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Removed</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Out of memory</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Generic error</td>
</tr>
<tr>
<td><strong>HiDiscovery Protocol Status</strong></td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>MRP Ring Redundancy Status</strong></td>
<td>1</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Not available</td>
</tr>
<tr>
<td><strong>Power Supply 1</strong></td>
<td>1</td>
<td>Present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Defective</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Not installed</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Power Supply 2</strong></td>
<td>1</td>
<td>Present</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Defective</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Not installed</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
The device operating as an OPC UA server processes the OPC UA information model data and transmits it securely to the OPC UA client application. The OPC UA server and OPC UA client communicate through a session.

The device operating as an OPC UA server shares the monitored data of the OPC UA information model. The user of the OPC UA client selects the items to be monitored in the OPC UA client application from a list of the IEC variables. The OPC UA client application requests the OPC UA information model data from the device operating as an OPC UA server using the specified OPC UA user account data.

The device sets up an OPC UA session by first negotiating the policy for a secure connection. Over this secure connection, the OPC UA client sends the login credentials of the OPC UA user account. The OPC UA server in the device then authenticates the OPC UA client. When the login credentials are valid, the device grants the OPC UA client access to its OPC UA Server function.

The device offers a role-based authentication and encryption concept to specifically control the access to its OPC UA server. The OPC UA client can use commands and functions associated with the OPC UA user account set up in the device.

**Table 48: Object values in the OPC UA information model**

<table>
<thead>
<tr>
<th>Object</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Power Down</td>
<td>1</td>
<td>Auto power down</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>No power save</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Energy efficient ethernet</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unsupported</td>
</tr>
<tr>
<td>Flow Control</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Disabled</td>
</tr>
<tr>
<td>Manual Cable Crossing</td>
<td>1</td>
<td>Medium dependent interface</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Medium dependent interface crossover</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Auto medium dependent interface crossover</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unsupported</td>
</tr>
<tr>
<td>Port On</td>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Testing</td>
</tr>
<tr>
<td>Power State</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Disabled</td>
</tr>
<tr>
<td>Send Trap</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Disabled</td>
</tr>
<tr>
<td>State</td>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td>Port Status</td>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Testing</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Dormant</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Not present</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Lower layer down</td>
</tr>
</tbody>
</table>

The device operating as an OPC UA server processes the OPC UA information model data and transmits it securely to the OPC UA client application. The OPC UA server and OPC UA client communicate through a session.

The device operating as an OPC UA server shares the monitored data of the OPC UA information model. The user of the OPC UA client selects the items to be monitored in the OPC UA client application from a list of the IEC variables. The OPC UA client application requests the OPC UA information model data from the device operating as an OPC UA server using the specified OPC UA user account data.

The device sets up an OPC UA session by first negotiating the policy for a secure connection. Over this secure connection, the OPC UA client sends the login credentials of the OPC UA user account. The OPC UA server in the device then authenticates the OPC UA client. When the login credentials are valid, the device grants the OPC UA client access to its OPC UA Server function.

The device offers a role-based authentication and encryption concept to specifically control the access to its OPC UA server. The OPC UA client can use commands and functions associated with the OPC UA user account set up in the device.
15.3.1 Enabling the OPC UA server

In the default setting, the OPC UA Server function is disabled. The Advanced > Industrial Protocols > OPC UA Server dialog lets you enable the OPC UA Server function. You can also specify the max. number of simultaneous OPC UA sessions. In the default setting, the values for the Listening port and Sessions (max.) fields are already specified. You specify the authentication and encryption protocol for OPC UA users at global level.

Perform the following steps:

- Open the Advanced > Industrial Protocols > OPC UA Server dialog.
- To enable the OPC UA Server function, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
- In the Listening port field, change the TCP port number, if necessary.
- In the Sessions (max.) field, change the number of OPC UA sessions that can be established simultaneously, if necessary.
- In the Security policy field, select the authentication and encryption protocol.
- Save the settings temporarily. To do this, click the ✓ button.
- To apply the changes, restart the OPC-UA server. Restart now? window.
- To apply the settings, click the Yes button.

```
enable
configure
opc-ua operation
opc-ua port <1..65535>
opc-ua sessions <1..5>

opc-ua security-policy none | basic128rsa15 | basic256 | basic256sha256
show opc-ua global
IEC62541 - OPC-UA server settings
--------------------------
IEC62541 - OPC-UA server operation............enabled
Listening port.........................4840
Number of concurrent sessions............5
Configured security-policy...............none
```
15.3.2 Setting up an OPC UA user account

The device lets you manage the OPC UA user accounts required to access the device using an OPC UA client application. Every OPC UA client user requires an active OPC UA user account to gain access to the OPC UA server of the device.

In the following example, we will set up an OPC UA user account for the OPC UA client user USER which has read access. Then the user USER is authorized to monitor the OPC UA information model data. To do this, perform the following steps:

1. Open the Advanced > Industrial Protocols > OPC UA Server dialog.
2. Click the button.
   The dialog displays the Create window.
3. Enter the name USER in the User name field.
4. Click the Ok button.
5. In the Password field, enter a password of at least 6 characters.
   In this example, we give the user account the password SECRET.
6. In the Access role column, select the readOnly item.
7. Save the settings temporarily. To do this, click the button.
   The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
8. To apply the settings, click the Yes button.
   The dialog displays the OPC UA user accounts that are set up.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access-Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>read-only</td>
<td>[x]</td>
</tr>
</tbody>
</table>

Note: When you set up a new OPC UA user account, remember to set the password.
15.3.3 **Deactivating an OPC UA user account**

After you deactivate the OPC UA user account, the user cannot access the device using the OPC UA Server function. Deactivating an OPC UA user account lets you keep the account settings and reuse them in the future. To do this, perform the following steps:

- Open the Advanced > Industrial Protocols > OPC UA Server dialog. The dialog displays the OPC UA user accounts that are set up.
- In the table row for the relevant OPC UA user account, unmark the checkbox in the Active column.
- Save the settings temporarily. To do this, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
- To apply the settings, click the Yes button.

```
enable
configure
opc-ua users disable USER
show opc-ua users
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To disable the user account USER.
To display the user accounts that are set up.

```
User Name       Access-Role  Status
----------------- ------------- -----
user             read-only   [ ]
save
```

To save the settings in the non-volatile memory (nvm) in the “selected” configuration profile.

15.3.4 **Delete an OPC UA user account**

To permanently deactivate the OPC UA user account settings, you delete the OPC UA user account. To do this, perform the following steps:

- Open the Advanced > Industrial Protocols > OPC UA Server dialog. The dialog displays the OPC UA user accounts that are set up.
- Select the table row of the relevant OPC UA user account.
- Click the button.
- Save the settings temporarily. To do this, click the ✓ button. The dialog displays the To apply the changes, restart the OPC/UA server. Restart now? window.
- To apply the settings, click the Yes button.

```
enable
configure
opc-ua users delete USER
```

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To delete the user account USER.
show opc-ua users

To display the user accounts that are set up.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access-Rrole</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

save

To save the settings in the non-volatile memory (nvm) in the "selected" configuration profile.
A Setting up the configuration environment

A.1 Setting up a DHCP/BOOTP server

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide if you want to purchase a license.

Perform the following steps:

☐ Install the DHCP server on your PC.
   To carry out the installation, follow the installation assistant.
☐ Start the haneWIN DHCP Server program.

![Start window of the haneWIN DHCP Server program](image)

**Note:** When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.

☐ In the menu bar, click the items Options > Preferences to open the program settings window.
☐ Select the DHCP tab.
☐ Specify the settings displayed in the figure.

![DHCP setting](image)

☐ Click the OK button.
☐ To enter the configuration profiles, click in the menu bar the items Options > Configuration Profiles.
Setting up the configuration environment

A.1 Setting up a DHCP/BOOTP server

- Specify the name for the new configuration profile.

![Figure 64: Adding configuration profiles](image)

- Click the **Add** button.
- Specify the netmask.

![Figure 65: Netmask in the configuration profile](image)

- Click the **Apply** button.
- Select the **Boot** tab.
- Enter the IP address of your tftp server.
- Enter the path and the file name for the configuration file.

![Figure 66: Configuration file on the tftp server](image)

- Click the **Apply** button and then the **OK** button.
- Add a profile for each device type.
  When devices of the same type have different configurations, you add a profile for each configuration.

![Figure 67: Managing configuration profiles](image)

- To complete the addition of the configuration profiles, click the **OK** button.
To enter the static addresses, in the main window, click the Static button.

Click the Add button.

Enter the MAC address of the device.

Enter the IP address of the device.

Select the configuration profile of the device.

Click the Apply button and then the OK button.

Add an entry for each device that will get its parameters from the DHCP server.
A.2 Setting up a DHCP server with Option 82

The following example describes the configuration of a DHCP server using the haneWIN DHCP Server software. This shareware software is a product of IT-Consulting Dr. Herbert Hanewinkel. You can download the software from www.hanewin.net. You can test the software for 30 calendar days from the date of the first installation, and then decide if you want to purchase a license.

Perform the following steps:
- Install the DHCP server on your PC.
  - To carry out the installation, follow the installation assistant.
- Start the haneWIN DHCP Server program.

![Figure 72: Start window of the haneWIN DHCP Server program](image)

**Note:** When Windows is activated, the installation procedure includes a service that is automatically started in the basic configuration. This service is also active although the program itself has not been started. When started, the service responds to DHCP queries.
Setting up the configuration environment
A.2 Setting up a DHCP server with Option 82

Figure 73: DHCP setting

☐ To enter the static addresses, click the Add button.

Figure 74: Adding static addresses

☐ Mark the Circuit Identifier checkbox.
☐ Mark the Remote Identifier checkbox.

Figure 75: Default setting for the fixed address assignment

☐ In the Hardware address field, specify the value Circuit Identifier and the value Remote Identifier for the switch and port.

The DHCP server assigns the IP address specified in the IP address field to the device that you connect to the port specified in the Hardware address field.

The hardware address is in the following form:
ci11hhvsvsmpprirlxxxxxxxxxxx

- ci
  Sub-identifier for the type of the Circuit ID
- cl
  Length of the Circuit ID.
- hh
  Hirschmann identifier:
  01 when a Hirschmann device is connected to the port, otherwise 00.
- vvvv
  VLAN ID of the DHCP request.
  Default setting: 0001 = VLAN 1
Socket of device at which the module with that port is located to which the device is connected. Specify the value 00.

- **mm** Module with the port to which the device is connected.
- **pp** Port to which the device is connected.
- **rl** Sub-identifier for the type of the Remote ID
- **rl** Length of the Remote ID
- **xxxxxxxxxxxx** Remote ID of the device (for example MAC address) to which a device is connected.

![Figure 76: Specifying the addresses](image)

![Figure 77: Application example of using Option 82](image)
A.3 Preparing access using SSH

You can connect to the device using SSH. To do this, perform the following steps:

- Generate a key in the device.
- or
- Transfer your own key onto the device.
- Prepare access to the device in the SSH client program.

Note: In the default setting, the key is already existing and access using SSH is enabled.

A.3.1 Generating a key in the device

The device lets you generate the key directly in the device. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- To disable the SSH server, select the off radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
- To create a RSA key, in the Signature frame, click the Create button.
- To enable the SSH server, select the On radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.

enable
configure
ssh key rsa generate

To change to the Privileged EXEC mode.
To change to the Configuration mode.
To generate a new RSA key.

A.3.2 Loading your own key onto the device

OpenSSH gives experienced network administrators the option of generating an own key. To generate the key, enter the following commands on your PC:

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

The device lets you transfer your own SSH key onto the device. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, SSH tab.
- To disable the SSH server, select the off radio button in the Operation frame.
- Save the settings temporarily. To do this, click the ✓ button.
- When the host key is located on your PC or on a network drive, drag and drop the file that contains the key in the up area. Alternatively click in the area to select the file.
Setting up the configuration environment

A.3 Preparing access using SSH

Perform the following steps:

- Copy the self-generated key from your PC to the external memory.
- Copy the key from the external memory into the device.

**A.3.3 Preparing the SSH client program**

The *PuTTY* program lets you access the device using SSH. You can download the software from [www.putty.org](http://www.putty.org).

Perform the following steps:

- Start the program by double-clicking on it.

![PuTTY input screen](image)

- In the *Host Name (or IP address)* field you enter the IP address of your device. The IP address (a.b.c.d) consists of 4 decimal numbers with values from 0 to 255. The 4 decimal numbers are separated by points.
- To select the connection type, select the *SSH* radio button in the *Connection type* option list.
- Click the *Open* button to set up the data connection to your device.

```bash
enable

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy sshkey envm &lt;file name&gt;</td>
<td>To load your own key onto the device from the external memory.</td>
</tr>
</tbody>
</table>
```

To change to the Privileged EXEC mode:

```bash
enable
```
Before the connection is established, the **PuTTY** program displays a security alarm message and lets you check the key fingerprint.

![Security alert prompt for the fingerprint](image)

Before the connection is established, the **PuTTY** program displays a security alarm message and lets you check the key fingerprint.

- Check the fingerprint of the key to help ensure that you have actually connected to the desired device.
- When the fingerprint matches your key, click the **Yes** button.

For experienced network administrators, another way of accessing your device through an SSH is by using the OpenSSH Suite. To set up the data connection, enter the following command:

```bash
ssh admin@10.0.112.53
```

**admin** is the user name.

**10.0.112.53** is the IP address of your device.
### A.4 HTTPS certificate

Your web browser establishes the connection to the device using the HTTPS protocol. The prerequisite is that you enable the HTTPS server function in the Device Security > Management Access > Server dialog, HTTPS tab.

**Note:** Third-party software such as web browsers validate certificates based on criteria such as their expiration date and current cryptographic parameter recommendations. Outdated certificates may cause issues due to invalid or outdated information. Example: An expired certificate or changed cryptographic recommendations. To solve validation conflicts with third-party software, transfer your own up-to-date certificate onto the device or regenerate the certificate with the latest firmware.

### A.4.1 HTTPS certificate management

A standard certificate according to X.509/PEM (Public Key Infrastructure) is required for encryption. In the default setting, a self-generated certificate is already present in the device. To do this, perform the following steps:

2. To create a X509/PEM certificate, in the Certificate frame, click the Create button.
3. Save the settings temporarily. To do this, click the ✓ button.
4. Restart the HTTPS server to activate the key. Restart the server using the Command Line Interface.

To change to the Privileged EXEC mode:
- `enable`

To change to the Configuration mode:
- `configure`

To generate a https X.509/PEM Certificate:
- `https certificate generate`

To disable the HTTPS function:
- `no https server`

To enable the HTTPS function:
- `https server`

The device also lets you transfer an externally generated X.509/PEM certificate onto the device:

2. When the certificate is located on your PC or on a network drive, drag and drop the certificate in the area. Alternatively click in the area to select the certificate.
3. Click on the Start button to copy the certificate to the device.
4. Save the settings temporarily. To do this, click the ✓ button.

To change to the Privileged EXEC mode:
- `enable`

To copy HTTPS certificate from external non-volatile memory device:
- `copy httpscert envm <file name>`
Setting up the configuration environment

A.4 HTTPS certificate

To activate the certificate after you created or transferred it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

A.4.2 Access through HTTPS

The default setting for HTTPS data connection is TCP port 443. If you change the number of the HTTPS port, then reboot the device or the HTTPS server. Thus the change becomes effective. To do this, perform the following steps:

- Open the Device Security > Management Access > Server dialog, HTTPS tab.
- To enable the function, select the On radio button in the Operation frame.
- To access the device by HTTPS, enter HTTPS instead of HTTP in your web browser, followed by the IP address of the device.

When you make changes to the HTTPS port number, disable the HTTPS server and enable it again in order to make the changes effective.

The device uses HTTPS protocol and establishes a new data connection. When you log out at the end of the session, the device terminates the data connection.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>no https server</td>
<td>To disable the HTTPS function.</td>
</tr>
<tr>
<td>https server</td>
<td>To enable the HTTPS function.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>To change to the Privileged EXEC mode.</td>
</tr>
<tr>
<td>configure</td>
<td>To change to the Configuration mode.</td>
</tr>
<tr>
<td>https port 443</td>
<td>To specify the number of the TCP port on which the web server receives HTTPS requests from clients.</td>
</tr>
<tr>
<td>https server</td>
<td>To enable the HTTPS function.</td>
</tr>
<tr>
<td>show https</td>
<td>To display the status of the HTTPS server and the port number.</td>
</tr>
</tbody>
</table>
Setting up the configuration environment

A.4 HTTPS certificate
B Appendix

B.1 Literature references

A small selection of books on network topics, ordered by publication date (newest first):

- **TSN – Time-Sensitive Networking (in German)**
  Wolfgang Schulte
  VDE Verlag, 2020
  ISBN 978-3-8007-5078-8

- **Time-Sensitive Networking For Dummies, Belden/Hirschmann Special Edition (in English)**
  Oliver Kleineberg and Axel Schneider
  Wiley, 2018
  Get your free PDF copy on [https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp](https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp)

- **IPv6: Grundlagen - Funktionalität - Integration (in German)**
  Silvia Hagen
  Sunny Connection, 3rd edition, 2016
  ISBN 978-3-9522942-3-9 (Print), ISBN 978-3-9522942-8-4 (eBook)

- **IPv6 Essentials (in English)**
  Silvia Hagen
  O'Reilly, 3rd edition, 2014

- **TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition) (in English)**
  W. R. Stevens and Kevin R. Fall
  Addison Wesley, 2011

- **Measurement, Control and Communication Using IEEE 1588 (in English)**
  John C. Eidson
  Springer, 2006

- **TCP/IP: Der Klassiker. Protokollanalyse. Aufgaben und Lösungen (in German)**
  W. R. Stevens
  Hüthig-Verlag, 2008
  ISBN 978-3-7785-4036-7

- **Optische Übertragungstechnik in der Praxis (in German)**
  Christoph Wrobel
  Hüthig-Verlag, 3rd edition, 2004
  ISBN 978-3-8266-5040-6
B.2 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at www.hirschmann.com.
B.3 Management Information Base (MIB)

The Management Information Base (MIB) is designed in the form of an abstract tree structure. The branching points are the object classes. The "leaves" of the MIB are called generic object classes.

When this is required for unique identification, the generic object classes are instantiated, that means the abstract structure is mapped onto reality, by specifying the port or the source address.

Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The object description or object ID (OID) identifies the object class. The subidentifier (SID) is used to instantiate them.

Example:

The generic object class `hm2PSState` (OID = 1.3.6.1.4.1.248.11.11.1.1.1.1.2) is the description of the abstract information power supply status. However, it is not possible to read any value from this, as the system does not know which power supply is meant.

Specifying the subidentifier 2 maps this abstract information onto reality (instantiates it), thus identifying it as the operating status of power supply 2. A value is assigned to this instance and can be read. The instance `get 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1` returns the response 1, which means that the power supply is ready for operation.

<table>
<thead>
<tr>
<th>Definition of the syntax terms used:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integer</strong></td>
</tr>
<tr>
<td><strong>IP address</strong></td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
</tr>
<tr>
<td><strong>Object Identifier</strong></td>
</tr>
<tr>
<td><strong>Octet String</strong></td>
</tr>
<tr>
<td><strong>PSID</strong></td>
</tr>
<tr>
<td><strong>TimeTicks</strong></td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
</tr>
<tr>
<td><strong>Type field</strong></td>
</tr>
<tr>
<td><strong>Counter</strong></td>
</tr>
</tbody>
</table>
When you have downloaded a software update from the product pages on the Internet, the ZIP archive of the device software also contains the MIBs.
### B.4 List of RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>768</td>
<td>UDP</td>
</tr>
<tr>
<td>783</td>
<td>TFTP</td>
</tr>
<tr>
<td>791</td>
<td>IP</td>
</tr>
<tr>
<td>792</td>
<td>ICMP</td>
</tr>
<tr>
<td>793</td>
<td>TCP</td>
</tr>
<tr>
<td>826</td>
<td>ARP</td>
</tr>
<tr>
<td>854</td>
<td>Telnet</td>
</tr>
<tr>
<td>855</td>
<td>Telnet Option</td>
</tr>
<tr>
<td>951</td>
<td>BOOTP</td>
</tr>
<tr>
<td>1112</td>
<td>IGMPv1</td>
</tr>
<tr>
<td>1157</td>
<td>SNMPv1</td>
</tr>
<tr>
<td>1155</td>
<td>SMIv1</td>
</tr>
<tr>
<td>1212</td>
<td>Concise MIB Definitions</td>
</tr>
<tr>
<td>1213</td>
<td>MIB2</td>
</tr>
<tr>
<td>1493</td>
<td>Dot1d</td>
</tr>
<tr>
<td>1542</td>
<td>BOOTP-Extensions</td>
</tr>
<tr>
<td>1643</td>
<td>Ethernet-like -MIB</td>
</tr>
<tr>
<td>1757</td>
<td>RMON</td>
</tr>
<tr>
<td>1867</td>
<td>Form-Based File Upload in HTML</td>
</tr>
<tr>
<td>1901</td>
<td>Community based SNMP v2</td>
</tr>
<tr>
<td>1905</td>
<td>Protocol Operations for SNMP v2</td>
</tr>
<tr>
<td>1906</td>
<td>Transport Mappings for SNMP v2</td>
</tr>
<tr>
<td>1945</td>
<td>HTTP/1.0</td>
</tr>
<tr>
<td>2068</td>
<td>HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03</td>
</tr>
<tr>
<td>2131</td>
<td>DHCP</td>
</tr>
<tr>
<td>2132</td>
<td>DHCP-Options</td>
</tr>
<tr>
<td>2233</td>
<td>The Interfaces Group MIB using SMI v2</td>
</tr>
<tr>
<td>2236</td>
<td>IGMPv2</td>
</tr>
<tr>
<td>2246</td>
<td>The TLS Protocol, Version 1.0</td>
</tr>
<tr>
<td>2346</td>
<td>AES Ciphersuites for Transport Layer Security</td>
</tr>
<tr>
<td>2365</td>
<td>Administratively Scoped IP Multicast</td>
</tr>
<tr>
<td>2578</td>
<td>SMIv2</td>
</tr>
<tr>
<td>2579</td>
<td>Textual Conventions for SMI v2</td>
</tr>
<tr>
<td>2580</td>
<td>Conformance statements for SMI v2</td>
</tr>
<tr>
<td>2613</td>
<td>SMON</td>
</tr>
<tr>
<td>2618</td>
<td>RADIUS Authentication Client MIB</td>
</tr>
<tr>
<td>2620</td>
<td>RADIUS Accounting MIB</td>
</tr>
<tr>
<td>2674</td>
<td>Dot1p/Q</td>
</tr>
<tr>
<td>2818</td>
<td>HTTP over TLS</td>
</tr>
<tr>
<td>2851</td>
<td>Internet Addresses MIB</td>
</tr>
<tr>
<td>2863</td>
<td>The Interfaces Group MIB</td>
</tr>
<tr>
<td>2865</td>
<td>RADIUS Client</td>
</tr>
<tr>
<td>2866</td>
<td>RADIUS Accounting</td>
</tr>
<tr>
<td>RFC 2868</td>
<td>RADIUS Attributes for Tunnel Protocol Support</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>RFC 2869</td>
<td>RADIUS Extensions</td>
</tr>
<tr>
<td>RFC 2869bis</td>
<td>RADIUS support for EAP</td>
</tr>
<tr>
<td>RFC 2933</td>
<td>IGMP MIB</td>
</tr>
<tr>
<td>RFC 3164</td>
<td>The BSD Syslog Protocol</td>
</tr>
<tr>
<td>RFC 3376</td>
<td>IGMPv3</td>
</tr>
<tr>
<td>RFC 3410</td>
<td>Introduction and Applicability Statements for Internet Standard Management Framework</td>
</tr>
<tr>
<td>RFC 3412</td>
<td>Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3413</td>
<td>Simple Network Management Protocol (SNMP) Applications</td>
</tr>
<tr>
<td>RFC 3414</td>
<td>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</td>
</tr>
<tr>
<td>RFC 3415</td>
<td>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3418</td>
<td>Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>RFC 3580</td>
<td>802.1X RADIUS Usage Guidelines</td>
</tr>
<tr>
<td>RFC 3584</td>
<td>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</td>
</tr>
<tr>
<td>RFC 3621</td>
<td>Power Ethernet MIB</td>
</tr>
<tr>
<td>RFC 4022</td>
<td>Management Information Base for the Transmission Control Protocol (TCP)</td>
</tr>
<tr>
<td>RFC 4113</td>
<td>Management Information Base for the User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td>RFC 4188</td>
<td>Definitions of Managed Objects for Bridges</td>
</tr>
<tr>
<td>RFC 4251</td>
<td>SSH protocol architecture</td>
</tr>
<tr>
<td>RFC 4291</td>
<td>IPv6 Addressing Architecture</td>
</tr>
<tr>
<td>RFC 4252</td>
<td>SSH authentication protocol</td>
</tr>
<tr>
<td>RFC 4253</td>
<td>SSH transport layer protocol</td>
</tr>
<tr>
<td>RFC 4254</td>
<td>SSH connection protocol</td>
</tr>
<tr>
<td>RFC 4293</td>
<td>Management Information Base for the Internet Protocol (IP)</td>
</tr>
<tr>
<td>RFC 4318</td>
<td>Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>RFC 4330</td>
<td>Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI</td>
</tr>
<tr>
<td>RFC 4363</td>
<td>Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions</td>
</tr>
<tr>
<td>RFC 4541</td>
<td>Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches</td>
</tr>
<tr>
<td>RFC 4836</td>
<td>Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)</td>
</tr>
<tr>
<td>RFC 4861</td>
<td>Neighbor Discovery for IPv6</td>
</tr>
<tr>
<td>RFC 5321</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>RFC 6221</td>
<td>Leightweight DHCPv6 Relay Agent</td>
</tr>
<tr>
<td>RFC 8200</td>
<td>IPv6 Specification</td>
</tr>
<tr>
<td>RFC 8415</td>
<td>DHCPv6</td>
</tr>
</tbody>
</table>
## B.5 Underlying IEEE Standards

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1AB</td>
<td>Station and Media Access Control Connectivity Discovery</td>
</tr>
<tr>
<td>IEEE 802.1D</td>
<td>MAC Bridges (switching function)</td>
</tr>
<tr>
<td>IEEE 802.1Q</td>
<td>Virtual LANs (VLANs, MRP, Spanning Tree)</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
<td>Port Authentication</td>
</tr>
<tr>
<td>IEEE 802.3</td>
<td>Ethernet</td>
</tr>
<tr>
<td>IEEE 802.3ac</td>
<td>VLAN Tagging</td>
</tr>
<tr>
<td>IEEE 802.3x</td>
<td>Flow Control</td>
</tr>
<tr>
<td>IEEE 802.3af</td>
<td>Power over Ethernet</td>
</tr>
</tbody>
</table>
### B.6 Underlying IEC Norms

<table>
<thead>
<tr>
<th>IEC 62439</th>
<th>High availability automation networks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MRP – Media Redundancy Protocol based on a ring topology</td>
</tr>
</tbody>
</table>
B.7 Underlying ANSI Norms

ANSI/TIA-1057  Link Layer Discovery Protocol for Media Endpoint Devices, April 2006
## B.8 Technical Data

### 15.3.5 Switching

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of the MAC address table (incl. static filters)</td>
<td>16384</td>
</tr>
<tr>
<td>Max. number of statically configured MAC address filters</td>
<td>100</td>
</tr>
<tr>
<td>Max. number of MAC address filters learnable through IGMP Snooping</td>
<td>512</td>
</tr>
<tr>
<td>Max. number of MAC address entries (MMRP)</td>
<td>64</td>
</tr>
<tr>
<td>Number of priority queues</td>
<td>8 Queues</td>
</tr>
<tr>
<td>Port priorities that can be set</td>
<td>0..7</td>
</tr>
<tr>
<td>MTU (Max. allowed length of packets a port can receive or transmit)</td>
<td>1996 Bytes</td>
</tr>
</tbody>
</table>

### 15.3.6 VLAN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID range</td>
<td>1..4042</td>
</tr>
<tr>
<td>Number of VLANs</td>
<td>max. 128 simultaneously per device</td>
</tr>
<tr>
<td></td>
<td>max. 128 simultaneously per port</td>
</tr>
</tbody>
</table>

### 15.3.7 Access Control Lists (ACL)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. number of ACLs</td>
<td></td>
</tr>
<tr>
<td>Max. number of rules per ACL</td>
<td></td>
</tr>
<tr>
<td>Max. number of rules per port</td>
<td></td>
</tr>
<tr>
<td>Number of total configurable rules</td>
<td></td>
</tr>
<tr>
<td>Max. number of VLAN assignments</td>
<td></td>
</tr>
<tr>
<td>Max. number of rules which log an event</td>
<td></td>
</tr>
<tr>
<td>Max. number of Ingress rules</td>
<td></td>
</tr>
</tbody>
</table>
B.9 Copyright of integrated Software

The product contains, among other things, Open Source Software files developed by third parties and licensed under an Open Source Software license.

You can find the license terms in the Graphical User Interface in the Help > Licenses dialog.
### B.10 Abbreviations used

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA</td>
<td>Name of the external memory</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>BOOTP</td>
<td>Bootstrap Protocol</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>Dynamic Host Configuration Protocol for IPv6</td>
</tr>
<tr>
<td>DUID</td>
<td>DHCP Unique Identifier</td>
</tr>
<tr>
<td>EUI</td>
<td>Extended Unique Identifier</td>
</tr>
<tr>
<td>FDB</td>
<td>Forwarding Database</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>LDRA</td>
<td>Lightweight DHCPv6 Relay Agent</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MRP</td>
<td>Media Redundancy Protocol</td>
</tr>
<tr>
<td>NDP</td>
<td>Neighbor Discovery Protocol</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comment</td>
</tr>
<tr>
<td>RM</td>
<td>Redundancy Manager</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
</tr>
<tr>
<td>SFTP</td>
<td>SSH File Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNTP</td>
<td>Simple Network Time Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TP</td>
<td>Twisted Pair</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
</tbody>
</table>
Appendix
B.10 Abbreviations used
# Index

## 0-9

802.1X ................................................................. 65

## A

Access roles .......................................................... 69  
Access security ..................................................... 111  
Advanced Information, MRP ..................................... 176  
Advanced Information, Sub Ring ................................. 210  
Advanced Mode ...................................................... 175, 177  
Aging time .............................................................. 139  
Alarm ................................................................. 221  
Alarm messages ...................................................... 219  
Alternate port ....................................................... 194, 200  
APNIC ................................................................. 42  
ARIN ................................................................. 42  
ARP ................................................................. 44  
Authentication list .................................................. 65  
Automatic configuration .......................................... 112

## B

Backup port .......................................................... 195, 200  
Bandwidth ............................................................. 154  
BOOTP ................................................................. 41  
BPDU ................................................................. 189  
BPDU guard ........................................................... 199, 200  
Bridge Identifier ..................................................... 186  
Bridge Protocol Data Unit .......................................... 189  

## C

CA certificate ........................................................ 254  
CIDR ................................................................. 44  
Classless inter domain routing .................................... 44  
Closed circuit ....................................................... 231  
Command Line Interface ........................................... 18  
Command tree ....................................................... 26  
Configuration file .................................................. 58  
Configuration modifications ....................................... 219
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D</strong></td>
</tr>
<tr>
<td>Data traffic ................................................. 123</td>
</tr>
<tr>
<td>Daylight saving time ................................. 85</td>
</tr>
<tr>
<td>Delay time (MRP) ........................................ 175</td>
</tr>
<tr>
<td>Denial of Service .................................. 123</td>
</tr>
<tr>
<td>Designated bridge ............................................. 194</td>
</tr>
<tr>
<td>Designated port ................................... 194, 199</td>
</tr>
<tr>
<td>Destination table .................................... 219</td>
</tr>
<tr>
<td>Device replacement ........................................ 15</td>
</tr>
<tr>
<td>Device status ..................................... 223</td>
</tr>
<tr>
<td>DHCP ............................................. 41</td>
</tr>
<tr>
<td>DHCP L2 Relay ......................................... 266</td>
</tr>
<tr>
<td>DHCP server ........................................... 84, 88, 299, 302</td>
</tr>
<tr>
<td>DHCPv6 ............................................ 59</td>
</tr>
<tr>
<td>Diameter (Spanning Tree) ......................... 188</td>
</tr>
<tr>
<td>DiffServ ............................................. 145</td>
</tr>
<tr>
<td>Disabled port .......................................... 195</td>
</tr>
<tr>
<td>DoS ................................................. 123</td>
</tr>
<tr>
<td>DSCP ............................................. 145, 152</td>
</tr>
<tr>
<td><strong>E</strong></td>
</tr>
<tr>
<td>Edge port ............................................... 194, 199</td>
</tr>
<tr>
<td>Email notification ..................................... 246</td>
</tr>
<tr>
<td>Event log ............................................ 254</td>
</tr>
<tr>
<td><strong>F</strong></td>
</tr>
<tr>
<td>FAQ .................................................. 331</td>
</tr>
<tr>
<td>First installation ....................................... 41</td>
</tr>
<tr>
<td>Flow control ......................................... 154</td>
</tr>
<tr>
<td><strong>G</strong></td>
</tr>
<tr>
<td>GARP .................................................. 272</td>
</tr>
<tr>
<td>Gateway .............................................. 42, 51</td>
</tr>
<tr>
<td>Generic object classes .......................... 313</td>
</tr>
<tr>
<td>Global Config mode .................................... 23, 24</td>
</tr>
<tr>
<td>GMRP ................................................. 272</td>
</tr>
<tr>
<td><strong>H</strong></td>
</tr>
<tr>
<td>HaneWin ............................................... 299, 302</td>
</tr>
<tr>
<td>Hardware reset ......................................... 219</td>
</tr>
<tr>
<td>HiDiscovery ........................................... 41</td>
</tr>
<tr>
<td>HiView ................................................ 64</td>
</tr>
<tr>
<td>Host address ........................................... 42</td>
</tr>
<tr>
<td><strong>I</strong></td>
</tr>
<tr>
<td>IANA .................................................. 42</td>
</tr>
<tr>
<td>IAS .................................................... 65</td>
</tr>
<tr>
<td>IEC 61850 .............................................. 280</td>
</tr>
<tr>
<td>IEEE 802.1X .......................................... 65</td>
</tr>
<tr>
<td>IEEE MAC address ..................................... 240</td>
</tr>
<tr>
<td>IGMP snooping ......................................... 139</td>
</tr>
<tr>
<td>Industrial HiVision .................................. 13</td>
</tr>
<tr>
<td>Instantiation ......................................... 313</td>
</tr>
<tr>
<td>Integrated authentication server ............ 65</td>
</tr>
<tr>
<td>IP address ............................................. 42, 51, 58</td>
</tr>
<tr>
<td>IP header ............................................... 145, 147</td>
</tr>
<tr>
<td>IPv6 address ............................................ 46</td>
</tr>
<tr>
<td>IPv6 address types .................................... 47</td>
</tr>
<tr>
<td>ISO/OSI layer model .................................. 44</td>
</tr>
<tr>
<td>L</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>M</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>O</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>P</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>RADIUS</td>
</tr>
<tr>
<td>RAM (memory)</td>
</tr>
<tr>
<td>Rapid Spanning Tree</td>
</tr>
<tr>
<td>Real time</td>
</tr>
<tr>
<td>Reconfiguration</td>
</tr>
<tr>
<td>Reconfiguration time (MRP)</td>
</tr>
<tr>
<td>Redundancy</td>
</tr>
<tr>
<td>Reference time source</td>
</tr>
<tr>
<td>Relay contact</td>
</tr>
<tr>
<td>Remote diagnostics</td>
</tr>
<tr>
<td>Report</td>
</tr>
<tr>
<td>Report message</td>
</tr>
<tr>
<td>RFC</td>
</tr>
<tr>
<td>Ring</td>
</tr>
<tr>
<td>Ring Manager</td>
</tr>
<tr>
<td>Ring manager</td>
</tr>
<tr>
<td>RIPE NCC</td>
</tr>
<tr>
<td>RM function</td>
</tr>
<tr>
<td>RMON probe</td>
</tr>
<tr>
<td>Root Bridge</td>
</tr>
<tr>
<td>Root guard</td>
</tr>
<tr>
<td>Root path</td>
</tr>
<tr>
<td>Root Path Cost</td>
</tr>
<tr>
<td>Root port</td>
</tr>
<tr>
<td>Router</td>
</tr>
<tr>
<td>Router Advertisement Daemon</td>
</tr>
<tr>
<td>RST BPDU</td>
</tr>
<tr>
<td>RSTP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure shell</td>
<td>18</td>
</tr>
<tr>
<td>Segmentation</td>
<td>219</td>
</tr>
<tr>
<td>Serial interface</td>
<td>18, 21</td>
</tr>
<tr>
<td>Service</td>
<td>251</td>
</tr>
<tr>
<td>Service shell</td>
<td>23</td>
</tr>
<tr>
<td>Service Shell deactivation</td>
<td>36</td>
</tr>
<tr>
<td>Setting the time</td>
<td>83</td>
</tr>
<tr>
<td>SFP module</td>
<td>239</td>
</tr>
<tr>
<td>Signal contact</td>
<td>231</td>
</tr>
<tr>
<td>SNMP</td>
<td>219</td>
</tr>
<tr>
<td>SNMP trap</td>
<td>219, 221</td>
</tr>
<tr>
<td>SNTP</td>
<td>83</td>
</tr>
<tr>
<td>Software version</td>
<td>105</td>
</tr>
<tr>
<td>SSH</td>
<td>18</td>
</tr>
<tr>
<td>Starting the graphical user interface</td>
<td>17</td>
</tr>
<tr>
<td>Store-and-forward</td>
<td>135</td>
</tr>
<tr>
<td>STP-BPU</td>
<td>189</td>
</tr>
<tr>
<td>Strict Priority</td>
<td>148</td>
</tr>
<tr>
<td>Sub Ring</td>
<td>172, 208</td>
</tr>
<tr>
<td>Sub Ring Advanced Information</td>
<td>210</td>
</tr>
<tr>
<td>Sub Ring Manager</td>
<td>217</td>
</tr>
<tr>
<td>Sub Ring Packet Prioritization</td>
<td>211</td>
</tr>
<tr>
<td>Sub Ring Packets</td>
<td>210</td>
</tr>
<tr>
<td>Sub Ring Redundant Manager</td>
<td>217</td>
</tr>
<tr>
<td>Subidentifier</td>
<td>313</td>
</tr>
<tr>
<td>Subnet</td>
<td>51</td>
</tr>
<tr>
<td>Syslog over TLS</td>
<td>254</td>
</tr>
<tr>
<td>System requirements (Graphical User Interface)</td>
<td>17</td>
</tr>
</tbody>
</table>
## Index

<table>
<thead>
<tr>
<th>T</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab Completion</td>
<td>33</td>
</tr>
<tr>
<td>TCN guard</td>
<td>200, 202</td>
</tr>
<tr>
<td>Technical questions</td>
<td>331</td>
</tr>
<tr>
<td>Topology Change flag</td>
<td>200</td>
</tr>
<tr>
<td>ToS</td>
<td>145, 147</td>
</tr>
<tr>
<td>Traffic class</td>
<td>148, 151</td>
</tr>
<tr>
<td>Training courses</td>
<td>331</td>
</tr>
<tr>
<td>Transmission reliability</td>
<td>200</td>
</tr>
<tr>
<td>Trap</td>
<td>219, 221</td>
</tr>
<tr>
<td>Trap destination table</td>
<td>219</td>
</tr>
<tr>
<td>Tree structure (Spanning Tree)</td>
<td>190, 193</td>
</tr>
<tr>
<td>Type of Service</td>
<td>147</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Exec mode</td>
<td>23</td>
</tr>
<tr>
<td>User name</td>
<td>19, 21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>148</td>
</tr>
<tr>
<td>VLAN</td>
<td>157</td>
</tr>
<tr>
<td>VLAN priority</td>
<td>150</td>
</tr>
<tr>
<td>VLAN tag</td>
<td>147, 157</td>
</tr>
<tr>
<td>VoIP</td>
<td>148</td>
</tr>
<tr>
<td>VT100</td>
<td>21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>W</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weighted Fair Queuing</td>
<td>148</td>
</tr>
<tr>
<td>Weighted Round Robin</td>
<td>148</td>
</tr>
</tbody>
</table>
D 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 www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

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 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 any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.
E  Readers’ Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

<table>
<thead>
<tr>
<th></th>
<th>Very Good</th>
<th>Good</th>
<th>Satisfactory</th>
<th>Mediocre</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precise description</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Readability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Understandability</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Examples</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Structure</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Graphics</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Drawings</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Tables</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

Did you discover any errors in this manual?
If so, on what page?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

Suggestions for improvement and additional information:
Dear User,

Please fill out and return this page
▶ as a fax to the number +49 (0)7127/14-1600 or
▶ per mail to
Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany