HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

DRAGON HiOS-2A Rel. 10.6.00



Reference Manual

Graphical User Interface

User Manual

Configuration

Security

HIRSCHMANN
A BELDEN BRAND

Reference Manual

Graphical User Interface
DRAGON Switch
HiOS-2A

Technical support
https://hirschmann-support.belden.com

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.

© 2026 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

Safety instructions . . . 9

About this Manual . . . 11

Key . . . 12

Notes on the Graphical User Interface . . . 13
Language Toggle . . . 13
Banner . . . 14
Menu pane . . . 15
Dialog area . . . 17

1 Basic Settings . . . 21
1.1 System . . . 21
1.2 Modules . . . 27
1.3 Network . . . 31
1.3.1 Global . . . 32
1.3.2 IPv4 . . . 34
1.3.3 IPv6 . . . 38
1.4 Out-of-Band . . . 42
1.5 Software . . . 45
1.6 Load/Save . . . 50
1.7 External Memory . . . 63
1.8 Port . . . 66
1.9 Restart . . . 73

2 Time . . . 75
2.1 Basic Settings . . . 75
2.2 Time Profile . . . 80
2.3 SNTP . . . 83
2.3.1 SNTP Client . . . 84
2.3.2 SNTP Server . . . 88
2.4 PTP . . . 90
2.4.1 PTP Global . . . 91
2.4.2 PTP Boundary Clock . . . 93
2.4.2.1 PTP Boundary Clock Global . . . 94
2.4.2.2 PTP Boundary Clock Port . . . 99
2.4.3 PTP Transparent Clock . . . 102
2.4.3.1 PTP Transparent Clock Global . . . 103
2.4.3.2 PTP Transparent Clock Port . . . 106

3 Device Security . . . 109
3.1 User Management . . . 109
3.2 Authentication List . . . 119
3.3 LDAP . . . 121
3.3.1 LDAP Configuration . . . 122
3.3.2 LDAP Role Mapping . . . 130

3.4 Management Access . . . 132
3.4.1 Server . . . 133
3.4.2 IP Access Restriction . . . 147
3.4.3 Web . . . 150
3.4.4 Command Line Interface . . . 151
3.4.5 SNMPv1/v2 Community . . . 153
3.5 Pre-login Banner . . . 155
3.6 SSH Known Hosts . . . 156

4 Network Security . . . 159
4.1 Network Security Overview . . . 159
4.2 Port Security . . . 161
4.3 802.1X . . . 167
4.3.1 802.1X Global . . . 168
4.3.2 802.1X Port Configuration . . . 172
4.3.3 802.1X Port Clients . . . 179
4.3.4 802.1X EAPOL Port Statistics . . . 181
4.3.5 802.1X Port Authentication History . . . 183
4.3.6 802.1X Integrated Authentication Server (IAS) . . . 185
4.4 RADIUS . . . 187
4.4.1 RADIUS Global . . . 189
4.4.2 RADIUS Authentication Server . . . 191
4.4.3 RADIUS Accounting Server . . . 195
4.4.4 RADIUS Authentication Statistics . . . 197
4.4.5 RADIUS Accounting Statistics . . . 199
4.5 DoS . . . 200
4.5.1 DoS Global . . . 201
4.6 DHCP Snooping . . . 204
4.6.1 DHCP Snooping Global . . . 206
4.6.2 DHCP Snooping Configuration . . . 208
4.6.3 DHCP Snooping Statistics . . . 211
4.6.4 DHCP Snooping Bindings . . . 212
4.7 IP Source Guard . . . 213
4.7.1 IP Source Guard Port . . . 215
4.7.2 IP Source Guard Bindings . . . 216
4.8 Dynamic ARP Inspection . . . 217
4.8.1 Dynamic ARP Inspection Global . . . 219
4.8.2 Dynamic ARP Inspection Configuration . . . 221
4.8.3 Dynamic ARP Inspection ARP Rules . . . 224
4.8.4 Dynamic ARP Inspection Statistics . . . 226
4.9 ACL . . . 227
4.9.1 ACL IPv4 Rule . . . 228
4.9.2 ACL MAC Rule . . . 236
4.9.3 ACL Assignment . . . 242

5 Switching . . . 245
5.1 Switching Global . . . 245
5.2 Rate Limiter . . . 247

5.3 Filter for MAC Addresses . . . 250
5.4 IGMP Snooping . . . 252
5.4.1 IGMP Snooping Global . . . 254
5.4.2 IGMP Snooping Configuration . . . 256
5.4.3 IGMP Snooping Enhancements . . . 260
5.4.4 IGMP Snooping Querier . . . 263
5.4.5 IGMP Snooping Multicasts . . . 266
5.5 MRP-IEEE . . . 267
5.5.1 MRP-IEEE Configuration . . . 268
5.5.2 MRP-IEEE Multiple MAC Registration Protocol . . . 269
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol . . . 274
5.6 GARP . . . 277
5.6.1 GMRP . . . 278
5.6.2 GVRP . . . 280
5.7 QoS/Priority . . . 281
5.7.1 QoS/Priority Global . . . 282
5.7.2 QoS/Priority Port Configuration . . . 283
5.7.3 802.1D/p Mapping . . . 285
5.7.4 IP DSCP Mapping . . . 287
5.7.5 Queue Management . . . 289
5.7.6 DiffServ . . . 290
5.7.6.1 DiffServ Overview . . . 292
5.7.6.2 DiffServ Global . . . 293
5.7.6.3 DiffServ Class . . . 294
5.7.6.4 DiffServ Policy . . . 301
5.7.6.5 DiffServ Assignment . . . 311
5.8 VLAN . . . 312
5.8.1 VLAN Global . . . 314
5.8.2 VLAN Configuration . . . 315
5.8.3 VLAN Port . . . 318
5.8.4 VLAN Voice . . . 320
5.8.5 MAC Based VLAN . . . 323
5.8.6 Subnet-based VLAN . . . 324
5.8.7 Protocol Based VLAN . . . 326
5.9 L2-Redundancy . . . 327
5.9.1 MRP . . . 329
5.9.2 HIPER Ring . . . 333
5.9.3 Spanning Tree . . . 334
5.9.3.1 Spanning Tree Global . . . 336
5.9.3.2 Spanning Tree MSTP . . . 343
5.9.3.3 Spanning Tree Port . . . 348
5.9.4 Link Aggregation . . . 357
5.9.5 Link Backup . . . 364
5.9.6 FuseNet . . . 367
5.9.6.1 Sub Ring . . . 368
5.9.6.2 Ring/Network Coupling . . . 373
5.9.6.3 Redundant Coupling Protocol . . . 379

6	**Diagnostics**	383
6.1	Status Configuration	383
6.1.1	Device Status	384
6.1.2	Security Status	389
6.1.3	Signal Contact	395
6.1.3.1	Signal Contact 1 / Signal Contact 2	396
6.1.4	MAC Notification	402
6.1.5	Alarms (Traps)	404
6.1.5.1	Trap V3 User Management	405
6.1.5.2	Trap Destinations	409
6.2	System	411
6.2.1	System Information	412
6.2.2	Hardware State	413
6.2.3	Configuration Check	414
6.2.4	IP Address Conflict Detection	416
6.2.5	ARP	420
6.2.6	Selftest	422
6.3	Email Notification	424
6.3.1	Email Notification Global	425
6.3.2	Email Notification Recipients	430
6.3.3	Email Notification Mail Server	432
6.4	Syslog	435
6.5	Ports	440
6.5.1	SFP	441
6.5.2	TP cable diagnosis	442
6.5.3	Port Monitor	444
6.5.4	Auto-Disable	454
6.5.5	Port Mirroring	458
6.5.6	RSPAN	462
6.6	LLDP	466
6.6.1	LLDP Configuration	467
6.6.2	LLDP Topology Discovery	471
6.7	Loop Protection	475
6.8	SFlow	479
6.8.1	SFlow Configuration	480
6.8.2	SFlow Receiver	482
6.9	Report	483
6.9.1	Report Global	484
6.9.2	Persistent Logging	488
6.9.3	System Log	491
6.9.4	Audit Trail	492
7	**Advanced**	493
7.1	DHCP	493
7.1.1	DHCP Server	493
7.1.1.1	DHCP Server Global	494
7.1.1.2	DHCP Server Pool	496

7.1.1.3 DHCP Server Lease Table . . . 503
7.2 DHCP L2 Relay . . . 504
7.2.1 DHCP L2 Relay Configuration . . . 505
7.2.2 DHCP L2 Relay Statistics . . . 508
7.3 DNS . . . 509
7.3.1 DNS Client . . . 509
7.3.1.1 DNS Client Global . . . 510
7.3.1.2 DNS Client Current . . . 511
7.3.1.3 DNS Client Static . . . 512
7.3.1.4 DNS Client Static Hosts . . . 515
7.3.2 OPC UA Server . . . 516
7.3.3 Service Discovery . . . 521
7.4 Tracking . . . 523
7.4.1 Tracking Configuration . . . 524
7.4.2 Tracking Applications . . . 528
7.5 Command Line Interface . . . 529

A Index . . . 531

B Technical support . . . 537

C Readers' Comments . . . 538

Safety instructions

⚠ WARNING

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, which is available in English only, contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Security” user manual, which is available in English only, introduces system security planning and policy development. It provides a detailed list of device security measures. It also describes how a secured device can improve the security and availability of your network. Its appendix contains details on hardware security seals and a password strength policy guide.

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:

• –	List item List item – second level
▶	Parameter value
☐	Task 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

Language Toggle

The Graphical User Interface of the device lets you toggle the display language. When you explicitly select the language on the login page, the web browser adds a `locale` parameter to the URL in the address bar, for example, `?locale=de`.

Without explicitly selecting a display language, the display language depends on the preferred language for web pages (also called website or content) in the web browser settings. For unsupported preferred languages, the device displays the Graphical User Interface in English (US).

The display language also determines the display format of dates and times.

Details:
- If the preferred language for web pages is German, the device displays the Graphical User Interface in German. This includes dates and times in the German format `DD.MM.YYYY, HH:MM:SS`.
  Example: `20.05.2026, 12:34:56`
- If the preferred language for web pages is other than German, the device displays the Graphical User Interface in English (US). This includes dates and times in the US format `MMM DD, YYYY, HH:MM:SS {AM|PM}`.
  Example: `May 20, 2026, 12:34:56 PM`

Banner

The banner displays the following information:



Displays or hides the menu pane.

Brand logo

Displays the brand logo.

Dialog name

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



Displays that the web browser 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 applied the settings, 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.

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 entry, this logs out the currently logged in user. Then the login dialog opens.

Menu pane

To display or hide 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 currently running device software that the device loaded during the last system startup.

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.

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

To display the collapsed menu tree again, click the button. The menu tree then displays only the menu items of the first 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:

- Read-only control elements
  - medium-dark border
  - light background (checkboxes, radio buttons)
  - shaded background (input fields)
- Editable control elements
  - dark border
  - light background

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 applied this modification. The modified settings are not yet effective.

Standard buttons

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



Applies the settings you modified 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 18.



Undoes the unsaved changes in the current dialog. Resets the values in the fields to the settings applied to the device.

Saving the settings

When applying settings, the device temporarily stores the modified settings. 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:

- Filtering table rows
- Sorting table rows
- Selecting multiple table rows

Filtering table 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.

Sorting table rows

You can change the order of the table rows. When you click the table header, an icon displays the sorting status.



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 ascending order based on the entries of the corresponding column. You might be able to restore the initial sorting in the table only after logging out and logging in again.



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 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 out and logging in again.

Selecting multiple table rows

You have the option of selecting multiple table rows at once and then apply an action to the selected table rows.
- ☐ 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.

Once you have selected multiple table rows, you can apply an action to each of these table rows at the same time, for example:
- Entering or changing the values in one table column
- Removing multiple table rows

1 Basic Settings

The menu contains the following dialogs:

- System
- Modules
- Network
- Out-of-Band
- Software
- Load/Save
- External Memory
- Port
- Restart

1.1 System

[Basic Settings > System]

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

Device status

Device status

Displays the device status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains 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 each 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 one power supply unit to a device that supports monitoring of 2 redundant power supply units, then the device triggers an alarm. To avoid this alarm, deactivate the monitoring of the missing power supply units in the *Diagnostics > Status Configuration > Device Status* dialog.

Security status



Security status

Displays the security status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains 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 each 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.



Signal contact status

Displays the signal contact status and the alarms that currently exist. When at least one alarm is present, the background color changes to red. Otherwise, the background color remains 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 each 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 generating an digital certificate, 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 hostname or Fully Qualified Domain Name (FQDN). For compatibility reasons, it is recommended to use only lowercase letters, as some systems differentiate uppercase from lowercase in the FQDN. Verify that this name is unique in the entire network.

- DHCP client
- *Syslog*

Location

Specifies the current or planned location.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  The device accepts the following characters:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Contact person

Specifies the contact person for this device.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  The device accepts the following characters:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

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*
- *not detected*
- *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 one device status alarm. For details, see the *Device status* frame.

Power

If the device supports 2 redundant power supply units: Only one supply voltage is active.

If the device supports one power supply unit: The supply voltage is active.

If the device supports 2 redundant power supply units: Both supply voltages are active.

RM

Redundancy Manager

- *MRP* ring manager

The device does not operate as a Redundancy Manager.

The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve.

The device operates as a Redundancy Manager. The redundancy function of the device is enabled but does not need the alternative connection at the moment. The redundancy reserve exists.

ACA

No external memory (*ENVM*) is connected.

The external memory (*ENVM*) is connected but not ready for operation.

The external memory (*ENVM*) is connected and ready for operation.

Port status

This frame displays a simplified view of the ports at the time of the last display update. You identify the port status from the indicator.

In the initial view, the frame only displays ports with an active link. When you click the button, the frame displays every port.

- The port speed is displayed next to the port number.
- When you hover the mouse pointer over or tap the appropriate port icon, a tooltip displays detailed port state information.

Green background color

Port with an active link.

Gray background color

Port with an inactive link.

Yellow background color

Port on which the device detected an unsupported SFP transceiver or an unsupported data rate.

Dashed border

Port in a *Blocking* state due to a redundancy function.

1.2 Modules

[Basic Settings > Modules]

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

The dialog contains the following tabs:
- [Ethernet module]
- [Fan module]
- [Power supply module]

[Ethernet module]

As long as the *Ethernet module status* column displays the value `configurable`, you can set up 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 into an empty slot, the device sets up 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 sets up the module with the default settings, and detects the module parameters.
- ☐ To update the Graphical User Interface, click the button.
  The *Ethernet module status* column displays the value `physical` for the installed Ethernet module.
- ☐ Apply the settings temporarily. To do this, click the button.

Activate/Deactivate a slot

On an inactive slot, the device recognizes the installed module and lets you set up the ports. The module establishes no network connections on an 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.
- ☐ Apply the settings temporarily. To do this, click the button.

Remove an Ethernet module

Perform the following steps:
- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the button.
  The *Ethernet module status* column displays the value `configurable` for the removed module.
- ☐ Select the table row of the removed module.

☐ Click the button.
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.

☐ Apply the settings temporarily. To do this, click the button.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 relates.

Active

Activates/deactivates the slot.

Possible values:

- marked (default setting)
  The slot is active. The device recognizes the 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 the number of ports that 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 setup.
- *remove*
  The slot is empty and inactive.
- *fix*
  The module cannot be removed.

[Fan module]

Operate the device only with the fan module installed. This helps prevent unwanted effects on the operation and lifespan of the device. If the module or a fan inside is inoperable, then replace the module immediately.

Install a module

Perform the following steps:

- ☐ Plug the module in the slot.
  The device automatically sets up the module with the default settings, and detects the module parameters.
- ☐ To update the Graphical User Interface, click the button.
  The *Fan module status* column displays the value *ok* for the installed module.

Uninstall a module

Perform the following steps:

- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the button.
  The *Fan module status* column displays the value *unavailable* for the removed module.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Fan module

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

Fan module status

Displays the status of the installed module.

Possible values:

- *unavailable*
  The module is not installed in the slot.
- *ok*
  The module is installed and operational.
- *failing*
  The module is installed, but an unexpected event occurred. For example, a fan in the module is inoperable.

[Power supply module]

The device has 2 module slots for power supply units and thus operates with redundant power supplies.

Install a module

Perform the following steps:

- ☐ Plug the module in the slot.
  The device automatically detects the module parameters.
- ☐ To update the Graphical User Interface, click the  button.
  The *Power supply status* column displays the value *present* or *not detected* for the installed module.

Uninstall a module

Perform the following steps:

- ☐ Remove the module from the slot.
- ☐ To update the Graphical User Interface, click the  button.
  The *Power supply status* column displays the value *not installed* for the removed module.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Power supply

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

Product code

Displays the product code of the installed module.

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

Version

Displays the version of the installed module.

A value of `0` indicates that the slot is empty.

Serial number

Displays the serial number of the installed module.

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

Power supply status

Displays the status of the installed module.

Possible values:

- *present*
  The module is installed and operational.
- *not detected*
  The module is installed, but an unexpected event occurred. For example, the module is not connected to the mains.
- *not installed*
  The module is not installed in the slot.

1.3 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- Global
- IPv4
- IPv6

1.3.1 Global

[Basic Settings > Network > 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.

MAC address

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

MAC address conflict detection

Enables/disables the *MAC address conflict detection* function.

Possible values:

- `marked`
  The *MAC address conflict detection* function is enabled.
  The device verifies that its MAC address is unique in the network.
- `unmarked` (default setting)
  The *MAC address conflict detection* function is disabled.

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.

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

[Basic Settings > Network > IPv4]

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

Configuration

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.

Management interface

VLAN ID

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

Possible values:

- `1..4042` (default setting: `1`)
  The drop-down list contains only those VLANs that are already set up in the *Switching > VLAN >* Configuration dialog.

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.
  or
  Select the *Do not modify VLAN port settings* item to retain the port VLAN settings. This option is useful if the VLANs are already set up.
- ☐ Click the *Ok* button.
  The device assigns the VLAN settings to the port:
  - 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 accessible through the selected port in the selected device management VLAN.

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

Verify that the IP subnet of the device management does not overlap with any subnet connected to another interface of the device:

- *Out-of-Band* management port

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

If the device does not use the specified gateway, then verify that another *default gateway* is specified. The setting in the following dialog has precedence:

- *Basic Settings > Out-of-Band* dialog, *Gateway address* field

BOOTP/DHCP

Client ID

Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is set up accordingly, then the server 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.

Lease time [s]

Displays the remaining time in seconds before the IP address, assigned to the device management by the DHCP server, expires.

To update the display, click the button.

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 Trivial File Transfer Protocol (TFTP). 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.

1.3.3 IPv6

[Basic Settings > Network > IPv6]

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

Operation

Operation

Enables/disables the IPv6 protocol in the device.

You can operate IPv4 and IPv6 simultaneously 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)
  IPv6 is enabled.
- *Off*
  IPv6 is disabled.
  If you want the device to operate only using IPv4, then disable IPv6 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 set up 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.

Management interface

VLAN ID

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

Possible values:

- `1..4042` (default setting: `1`)
  The drop-down list contains only those VLANs that are already set up in the *Switching > VLAN > Configuration* dialog.

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.
  or
  Select the *Do not modify VLAN port settings* item to retain the port VLAN settings. This option is useful if the VLANs are already set up.
- ☐ Click the *Ok* button.
  The device assigns the VLAN settings to the port:
  - 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 accessible through the selected port in the selected device management VLAN.

DHCP

Client ID

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

The IPv6 address received from the DHCPv6 server has the *PrefixLength* value `128`. According to RFC 8415, a DHCPv6 server cannot currently 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 set up for the device management.

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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, an IPv6 address does not use a subnet mask to identify the subnet part of the 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 specified. 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 sets up 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

[Basic Settings > Out-of-Band]

The device has a *Service 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 the *Service Port* network interface to access the device management.

The device lets you access the device management through the *Service Port* network interface using the following protocols:
- HTTP
- HTTPS
- SSH
- Telnet
- SNMP
- FTP
- TFTP
- SFTP
- SCP

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

Operation

Operation

Enables/disables the *Service Port* network interface.

Possible values:
- *On* (default setting)
  The device lets you access the device management through the *Service Port* network interface.
- *Off*
  The device prohibits access to the device management through the *Service Port* network interface.

Management interface

IP address assignment

Specifies the source from which the device management receives its IP parameters for access through the *Service Port* network interface.

Possible values:

- `Local` (default setting)
  The device management uses the IP parameters specified in the *IP parameter* frame.
- `DHCP`
  The device management uses an external DHCP server to assign the IP parameters to the *Service Port* network interface.
  When the DHCP server also provides DNS server addresses, the device displays these addresses in the *Advanced > DNS > Client > Current* dialog.
  If there is no response from the DHCP server, then the device sets the IP address to `0.0.0.0` and makes another attempt to obtain a valid IP address.

MAC address

Displays the MAC address of the *Service Port* network interface.

Status

Displays the operating status of the *Service Port* network interface.

IP parameter

Verify that the IP subnet of this network interface does not overlap 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 *Service Port* network interface.

Possible values:

- Valid IPv4 address
  (default setting: `192.168.1.1`)

Netmask

Specifies the netmask.

Possible values:

- Valid IPv4 netmask
  (default setting: `255.255.255.0`)

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
  (default setting: `0.0.0.0`)
  Verify that *IP address* and *Gateway address* are in the same network.

This setting takes precedence over the *default gateway* setting in the *Basic Settings > Network > IPv4* dialog, *Gateway address* field.

Remaining lease time

Lease time [s]

Displays the remaining time in seconds before the IP address, assigned to the device management by the DHCP server out-of-band through the *Service Port*, expires.

To update the display, click the button.

1.5 Software

[Basic Settings > 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 that is saved in the device.

Note:
Before you update 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 currently running device software that the device loaded during the last system startup.

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

The device swaps the device software images and accordingly the values displayed in the fields *Stored version* and *Backup version*.

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

The device lets you update the device software at this place, if a suitable device software image is available outside the device. If a suitable device software image is saved on the selected external memory (*ENVM*), use the table in the *File system* tab below.

URL

Specifies the path and the file name of the device software image that you use to update the device software.

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

- Software update from the PC

  Drag and drop the file into the ⬆ area from your PC or network drive. As an alternative, click in the area to select the file.
- Software update through FTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on an FTP server, then specify the URL in the following form:
  `ftp://<user>:<password>@<IP address>[:port]/<file name>`
- Software update through TFTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on a TFTP server, then specify the URL in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Software update through SCP or SFTP
  If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Updates the device software.

- To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the *Device Security > Management Access > Web* dialog, *Web interface session timeout [min]* field.
- The device transfers the previously used device software to the backup memory.
- The device transfers the selected file to the flash memory, replacing the previously used device software. During the next startup, the device boots with the device software that you have transferred.

Allow upload of unsigned device software

Activates/deactivates the option that the device allows to upload an unsigned device software. The purpose of this setting is to enable the upload of a device software that does not have a cryptographic signature.

Possible values:

- `marked`
  The device allows to upload an unsigned device software.
  Uploading an unsigned device software can be a security risk. If you trust the originator, then you can upload the unsigned device software.
- `unmarked` (default setting)
  The device only allows to upload a signed device software.

Secure Boot enabled

Activates a mode in which the device only boots with a device software image that has a valid cryptographic signature.

Possible values:

- `marked`
  During system startup, the device only boots with a device software image that has a valid cryptographic signature.
  Once activated, you cannot deactivate the mode:
  - The checkbox is permanently grayed out.
  - You cannot downgrade to a software version earlier than 10.3.00.
  - The *Allow upload of unsigned device software* checkbox is permanently hidden.
- `unmarked` (default setting)
  During system startup, the device boots with any device software image, whether the device software image is cryptographically signed or not. However, in case of a cryptographically signed device software image, its signature has to be valid.

[File system]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Update Firmware

Updates the device software if a suitable device software image is saved on the selected external memory (*ENVM*). The prerequisite is that a table row is selected for which the *File location* column displays the value *sd-card* or *usb*.

- Verify that the relevant external memory is selected from the *Selected external memory* drop-down list. See the *Basic Settings > Load/Save* dialog, *External memory* frame.
- To remain logged in to the device management during the software update, move the mouse pointer occasionally. As an alternative, before you start the software update, specify a sufficiently high value in the *Device Security > Management Access > Web* dialog, *Web interface session timeout [min]* field.
- The device transfers the previously used device software to the backup memory.
- The device transfers the selected file to the flash memory, replacing the previously used device software. During the next startup, the device boots with the device software that you have transferred.

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
- *sd-card*
  External SD memory (ACA31)
- *usb*
  External USB memory (ACA22)

Index

Displays the index of the device software.

The index number of the device software in the flash memory 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

[Basic Settings > 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

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Remove

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

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

Save

Saves the temporarily applied settings in 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 saves a copy of the configuration profile in the external memory (*ENVM*).

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

Save as...

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*).

- ☐ Click the *Profile name* drop-down list and enter in the search box the name for saving the configuration profile (maximum 32 characters).
  - ☐ To overwrite an existing configuration profile, select the desired item from the search results.
  - ☐ To save the configuration profile with a new name, click the *Create* link below the search box.

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 adding 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 factory 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 selected external memory (*ENVM*). See the *External memory* frame.

☐ 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 it onto the ⬆ area. As an alternative, click in the area to select the file.
- – Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on an FTP server, then specify the URL in the following form:
  `ftp://<user>:<password>@<IP address>[:port]/<file name>`
- – Import through TFTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on a TFTP server, then specify the URL in the following form:
  `tftp://<IP address>/<path>/<file name>`
- – Import through SCP or SFTP
  If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
  `scp://` or `sftp://<IP address>/<path>/<file name>`
  Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

☐ 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* 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 through FTP
  Do not use this method if you transmit data over untrusted networks.
  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 through TFTP
  Do not use this method if you transmit data over untrusted networks.
  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 through SCP or SFTP
  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>`
    Click the *Ok* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

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 from 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 it onto the area. As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on an FTP server, then specify the URL in the following form:
  `ftp://<user>:<password>@<IP address>[:port]/<file name>`
- Import through TFTP
  Do not use this method if you transmit data over untrusted networks.
  If the file is on a TFTP server, then specify the URL in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
  `scp://` or `sftp://<IP address>/<path>/<file name>`
  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Back to factory...

Resets the device settings 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 digital 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 (*ENVM*) is connected, the device deletes the configuration profiles saved in the external memory.
- After a short time, the device reboots and then uses the default settings.

Back to default

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

Storage

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.
- *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.

Last modified (UTC)

Displays the Universal Time Coordinated (UTC) time 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 applied settings in this configuration profile.
- `unmarked`
  Another configuration profile is designated as “Selected”.

Encryption

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.

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.

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.

External memory

Selected external memory

Specifies the external memory that the device uses for file operations.

This setting has the following effects:

- For example, the device stores a copy of the device configuration files on the selected external memory (*ENVM*).
- The device lets you conveniently update the device software if a suitable device software image is saved on the selected external memory (*ENVM*). See the *Basic Settings > Software* dialog.

Possible values:

- *sd*
  External SD memory (ACA31)
- *usb*
  External USB memory (ACA22)

Status

Displays the operating state of the selected external memory (*ENVM*).

Possible values:

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

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* or *second* 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:

- ☐ 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.
- ☐ In the *New password* field, enter the password.
  To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox.
- ☐ 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 (*ENVM*).

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 adding 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 inoperable device, then perform the following steps:

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

Note:
The prerequisite for loading a configuration profile from the external memory (*ENVM*) is that in the *Basic Settings > External Memory* dialog the *Config priority* column displays the value *first* or *second*. This value is set as the default setting.

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 (*ENVM*).

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 (*ENVM*) 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 (*ENVM*) 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
  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

The device gives you the following options for backing up the file onto the remote server:

- Backup through FTP
  Do not use this method if you transmit data over untrusted networks.
  To back up the file to an FTP server, specify the URL for the file in the following form:
  `ftp://<IP address>[:port]/<path>/<file name>`
- Backup through TFTP
  Do not use this method if you transmit data over untrusted networks.
  To back up the file to a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Backup through SCP or SFTP
  To back up the file to an SCP or SFTP server, specify the URL for the file in the following form:
  - `scp://` or `sftp://<IP address>/<path>/<file name>`
    Click the *Start* button to open the *Credentials* window.

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

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`
    `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

1.7 External Memory

[Basic Settings > 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 18.

Type

Displays the type of the external memory (*ENVM*).

Possible values:

- *sd*
  External SD memory (ACA31)
- *usb*
  External USB memory (ACA22)

Status

Displays the operating state of the external memory (*ENVM*).

Possible values:

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

Writable

Displays if the device has write access to the external memory (*ENVM*).

Possible values:

- marked
  The device has write access to the external memory (*ENVM*).
- unmarked
  The device has read-only access to the external memory (*ENVM*). 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 (*ENVM*):
  - the device software image file
  - a text file `startup.txt` with the content `autoUpdate=<software_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 the external memory (*ENVM*) 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 (*ENVM*) 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*, *second*
  The device loads the configuration profile from the external memory (*ENVM*) designated as *first*.
  When the device does not find a configuration profile there, it loads the configuration profile from the external memory (*ENVM*) designated as *second*, and so on.
  When the device does not find a configuration profile in the external memory (*ENVM*), 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* or *second* 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 saving a copy of the configuration profile in the external memory (*ENVM*).

Possible values:

- `marked` (default setting)

  Saving a copy is activated. When you click in the *Basic Settings > Load/Save* dialog the button, the device saves a copy of the configuration profile on the active external memory (*ENVM*).
- `unmarked`

  Saving a copy is deactivated. The device does not save 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

[Basic Settings > 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]
- [Ingress Utilization]

[Configuration]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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.
  If the port is disabled even though the *Port on* checkbox is marked, it means that the port was disabled by another function, for example *Auto-Disable* or *Port Monitor*. You specify the settings of the *Auto-Disable* function in the *Diagnostics > Ports > Auto-Disable* dialog. You specify the settings of the *Port Monitor* function in the *Diagnostics > Ports > Port Monitor* dialog.

Autoneg

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

Possible values:

- `marked` (default setting for twisted-pair ports)
  The automatic selection of the operating mode is active.
  The port negotiates the operating mode independently using auto-negotiation and automatically detects the assignment of the twisted-pair port connectors (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* column.
- Grayed-out display (default setting for optical ports with port speeds > `1G`)
  No automatic selection of the operating mode.

Manual configuration

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

Possible values:

- `10M FDX`
  Full-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection
- `10G 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.
- `10M FDX`
  Full-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection
- `2.5G FDX`
  Full-duplex connection
- `10G 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

Specifies the devices connected to a twisted-pair port.

The prerequisite is that the *Autoneg* function is disabled.

Possible values:

- *mdi*
  The device interchanges the send- and receive-line pairs on the port.
- *mdix* (default setting on twisted-pair ports)
  The device helps prevent the interchange of the send- and receive-line pairs on the 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 over a crossed cable, the device automatically resets the port from *mdix* to *mdi*.
- *unsupported* (default setting on optical ports or twisted-pair 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) 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 interruptions 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 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

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.

MTU

Specifies the maximum allowed size of Ethernet packets on the port in bytes.

Possible values:

- `1518..12288` (default setting: `1518`)
  With the setting `1518`, the port transmits the Ethernet packets up to the following size:
  - 1518 bytes without VLAN tag
    (1514 bytes + 4 bytes CRC)
  - 1522 bytes with VLAN tag
    (1518 bytes + 4 bytes CRC)

This setting lets you increase the max. allowed size of Ethernet packets that this port can receive or transmit.

The following list contains possible applications:

- When you use the device in the transfer network with double VLAN tagging, it is possible that you require an *MTU* that is larger by 4 bytes.

On other interfaces, you specify the maximum permissible size of the Ethernet packets as follows:

- *Link Aggregation* interfaces
  Switching > L2-Redundancy > Link Aggregation dialog, *MTU* column

Power state

Specifies if the port is physically enabled or disabled after you deactivated the port in the *Port on* column.

Possible values:

- `marked`
  The device keeps the port physically enabled when the *Port on* checkbox is unmarked. A device connected to this port continues to detect the link status as active.
- `unmarked` (default setting)
  The port is physically disabled. The physical status of the port is controlled only by the setting in the *Port on* column.

Track name

Specifies the name of the tracking object to which the device links the physical port.

The prerequisite is that in the *Advanced > Tracking > Configuration* dialog, the *Track name* field is already set up.

Possible values:

- `<Track name>` (default setting: `-`)
  The device automatically activates or deactivates the link status of a physical port depending on the selected tracking object from the drop-down list.

Power save

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.

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 unicasts*
  - *Received multicasts*
  - *Received broadcasts*
- Number of data packets/bytes sent or forwarded by the device
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicasts*
  - *Transmitted multicasts*
  - *Transmitted broadcasts*
- 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.
or
☐ In the *Basic Settings > Restart* dialog, click the *Clear port statistics* button.

[Ingress Utilization]

This tab displays the ingress network load on the individual ports.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

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 between the received data quantity and the maximum possible data quantity at the currently set data rate.

Lower threshold [%]

Specifies the lower notification threshold value for the network load. If the network load on the port falls below this value, then the status of the checkbox in the *Alarm* column changes to `marked`.

Possible values:

- `0.00..100.00` (default setting: `0.00`)

The value `0` or `0.00` deactivates the lower notification threshold value.

Upper threshold [%]

Specifies the upper notification threshold value for the network load. If the network load on the port exceeds this value, then the status of the checkbox in the *Alarm* column changes to `marked`.

Possible values:

- `0.00..100.00` (default setting: `0.00`)

The value `0` or `0.00` deactivates the upper notification threshold value.

Control interval [s]

Specifies the interval in seconds by which the device determines and possibly limits the network load.

Possible values:

- `1..3600` (default setting: `30`)

Alarm

Displays the utilization alarm status.

Possible values:

- `marked`
  The network load on 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 network load on the port is between the lower and the upper notification threshold values.

1.9 Restart

[Basic Settings > Restart]

This dialog lets you restart the device, reset port counters and the MAC address table (forwarding database), and delete log files.

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 elapses, the device restarts and goes through the following phases:

- If you activate the function in the *Diagnostics > System > Selftest* dialog, then the device performs the RAM self-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.

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.

Buttons

Clear FDB

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.

Clear 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 the device management access statistics to `0`.

See the *Diagnostics > System > System Information* dialog, `Used Management Ports` table.

Clear 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.

Clear log file

Removes the logged events from the log file.

See the *Diagnostics > Report > System Log* dialog.

Clear persistent log file

Removes the log files from the external memory (*ENVM*).

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
- Time Profile
- SNTP
- PTP

2.1 Basic Settings

[Time > Basic Settings]

The device is equipped with a buffered hardware clock. This clock keeps the correct time if the power supply becomes inoperable, or you disconnect the device from the power supply. After the system startup, the correct time is available again, 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 continuously 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]

Note:
The display format of dates and times is determined by the Graphical User Interface language. You can toggle the language, see “Language Toggle” on page 13.

[Global]

In this tab, you specify the system time and the time zone.

Configuration

System time (UTC)

Displays the date and time as Universal Time Coordinated (UTC), that is, without the value specified in the *Local offset [min]* field.

Set time from PC

The device takes over the time from your management station as the system time.

System time

Displays the local date and time: *System time* = *System time (UTC)* + *Local offset [min]* + *Daylight saving time*

Time source

Displays the time source from which the device obtains 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. See the *Time > SNTP* dialog.
- `ptp`
  The *PTP* function is enabled, and the device clock is synchronized with a *PTP master clock*. See the *Time > PTP* dialog.

Local offset [min]

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

Possible values:

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

[Daylight saving time]

In this tab, you enable/disable the *Daylight saving time* function. You specify the start and end of summer time using a pre-defined profile. As an alternative, you specify these settings individually. During the summer time, the device advances the local time by one 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 sets the clock forward to summer time and back again.
- `Off` (default setting)
  The *Daylight saving time* mode is disabled.

You specify the daylight saving time settings in the *Summertime begin* and *Summertime end* frames.

Profile...

Opens the *Profile...* window to select a pre-defined profile for the start and end of summer time. Selecting a profile overwrites the settings specified in the *Summertime begin* and *Summertime end* frames.

Possible values:

- *EU*
  Daylight saving time settings as applicable in the European Union.
- *USA*
  Daylight saving time settings as applicable in the United States.

Summertime begin

In this frame, you specify the time at which the device sets the clock forward from standard time to summer time. In the first 3 fields, you specify the day for the start of summer time. In the last field, you specify the time.

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 at which the device sets the clock forward to summer time.

Possible values:

- `<HH:MM>` (default setting: `00:00`)

Summertime end

In this frame, you specify the time at which the device resets the clock from summer time to standard time. In the first 3 fields, you specify the day for the end of summer time. In the last field, you specify the time.

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 at which the device resets the clock to standard time.

Possible values:

- `<HH:MM>` (default setting: `00:00`)

2.2 Time Profile

[Time > Time Profile]

This dialog lets you set up time profiles. If you assign a time profile, for example, to an ACL rule, then the device applies the rule at the times specified in the time profile.

The device lets you set up to 100 time profiles.
- If a time profile is assigned to a rule, the device applies the rule during the times specified within the time profile.
- If no time profile is assigned to a rule, the device applies the rule permanently.

Each time profile can contain:
- One *Absolute* time period and up to 9 *Periodic* time periods
  or
- Up to 10 *Periodic* time periods

Note:
The display format of dates and times is determined by the Graphical User Interface language. You can toggle the language, see “Language Toggle” on page 13.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Note:
If you reconfigure a time period, then first specify the end time and then the start time. Otherwise, the dialog displays an error message.

Buttons

 Add

Opens the *Create* window to add a time period.
- From the *Profile name* drop-down list, you select the name of the time profile to which the time period belongs or add a new name.
  Enter the name in the search box.
  - ☐ To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  - ☐ To add a name: Enter the name in the search box, then click the *Create* link below the search box.
- In the *Type* field, you specify the type of time period.
  - With the *Periodic* radio button, you specify a time period during which the device activates the recurring rule.
  - With the *Absolute* radio button, you specify a time period during which the device activates the rule one time. Within every time profile, exactly one such time period is allowed.

 Remove

Removes the selected table row.

Profile name

Displays the name of the time profile. The time profile contains the time periods.

Operational status

Displays whether the status of the time profile is currently *active* or *inactive*.

Index

Displays the number of the time period within the time profile. The device automatically assigns the value when you add a table row.

Type

Displays the time profile type.

Possible values:

- `Absolute`
  The device applies the rule once. For more information, refer to columns *Start date* to *End time*.
- `Periodic`
  The device applies the rule recurrently. For more information, refer to columns *Start days* to *End time*.

Absolute

Start date

Specifies the date at which the device starts to apply the one-time rule.

Possible values:

- `<Day of the week, date>`
  (depending on the language and region settings of your computer)

Start time

Specifies the time at which the device starts to apply the one-time rule.

Possible values:

- `hh:mm AM/PM`
  Hour:Minute

End date

Specifies the date at which the device terminates the one-time rule.

Possible values:

- `<Day of the week, date>`
  (depending on the language and region settings of your computer)

The device also allows you to specify time periods that span several days.

Example:

- *Start date*: *Sat*
- *Start time*: `12:00 PM`

- *End date*: *Sun*
- *End time*: `11:00 AM`

End time

Specifies the time at which the device terminates the one-time rule.

Possible values:

- `hh:mm AM/PM`
  Hour:Minute

Periodic

Start days

Specifies the days of the week on which the device periodically starts to apply the rule.

The device allows you to specify multiple values in the *Start days* column, for example a list of the weekdays *Mon*,*Tue*,*Wed*,*Thu*,*Fri*. In this case, verify that the *Start days* and *End days* fields contain identical values. The device then applies the rule every weekday at the times specified in the *Start time* and *End time* fields.

Possible values:

- *Sun*
- *Mon*
- *Tue*
- *Wed*
- *Thu*
- *Fri*
- *Sat*

Start time

Specifies the time at which the device periodically starts to apply the rule.

Possible values:

- `hh:mm AM/PM`
  Hour:Minute

End days

Specifies the days of the week on which the device periodically terminates the rule.

The device allows you to specify multiple values in the *End days* column, for example a list of the weekdays *Mon*,*Tue*,*Wed*,*Thu*,*Fri*. In this case, verify that the *Start days* and *End days* fields contain identical values. The device then applies the rule every weekday at the times specified in the *Start time* and *End time* fields.

The device also allows you to specify time periods that span several days. In this case, verify that the *Start days* and *End days* fields each contain a single value.

Example: *Start days*: *Sat*, *Start time*: `12:00 PM`, *End days*: *Sun*, *End time*: `11:00 AM`

Possible values:

- *Sun*
- *Mon*
- *Tue*
- *Wed*
- *Thu*
- *Fri*
- *Sat*

End time

Specifies the time at which the device periodically terminates the rule.

Possible values:

- `hh:mm AM/PM`
  Hour:Minute

2.3 SNTP

[Time > SNTP]

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

With the SNTP client function, the device lets you synchronize the local system clock with an external NTP or SNTP server.

As the SNTP server, the device makes the time information available to other devices in the network.

The menu contains the following dialogs:

- SNTP Client
- SNTP Server

2.3.1 SNTP Client

[Time > 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 time information from an external NTP or SNTP servers and synchronizes the local system clock with the time from the time server.

Operation

Operation

Enables/disables the *Client* function in the device. Note the setting in the *Disable client after successful sync* checkbox in the *Configuration* frame.

Possible values:

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

State

State

Displays the status of the *Client* function.

Possible values:

- *disabled*
  The SNTP client is not operating.
- *notSynchronized*
  The SNTP client is operating.
  The local system clock is not in sync with an external NTP or SNTP server.
- *synchronizedToRemoteServer*
  The SNTP client is operating.
  The local system clock is in sync with an external NTP or SNTP server.

Configuration

Mode

Specifies if the device actively requests the time information from an external NTP or SNTP server set up in the device (*unicast* mode) or passively waits for the time information from a random NTP or SNTP server (*broadcast* mode).

Possible values:

- *unicast* (default setting)
  The device takes the time information only from one of the set-up NTP or SNTP servers. The device sends Unicast requests to the external SNTP or NTP server and evaluates the response of the server.
- *broadcast*
  The device obtains the time information from a random NTP or SNTP server. The device evaluates the Broadcasts or Multicasts from this server.

Request interval [s]

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

Possible values:

- `5..3600` (default setting: `30`)

Broadcast recv timeout [s]

Specifies the time in seconds the device operating in *broadcast* mode waits before changing the value in the *State* field from *syncToRemoteServer* to *notSynchronized* when it does not receive Broadcast packets. See the *State* frame.

Possible values:

- `128..2048` (default setting: `320`)

Disable client after successful sync

Activates/deactivates the automatic disabling of the *SNTP Client* function after the device has successfully synchronized its local system clock.

Possible values:

- `marked`
  The automatic disabling of the *SNTP Client* function is active.
  The device disables the *SNTP Client* function after it has successfully synchronized its local system clock.
- `unmarked` (default setting)
  The automatic disabling of the *SNTP Client* function is inactive.
  The device keeps the *SNTP Client* function enabled after it has successfully synchronized its local system clock.

Table

In the table, you specify the settings for up to 4 external NTP or SNTP servers. After enabling the function, the device sends requests to the server set up in the first table row.

When the external NTP or SNTP server does not respond, the device sends its request to the server set up in the next table row. When the device does not receive a response, it cyclically sends requests to each set-up NTP or SNTP server until it receives a valid time from one of these servers. The device synchronizes its local system clock with the first responding NTP or SNTP server, even if an server ahead in the table will be reachable again later.

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 add a table row, the device fills the first gap.

Name

Specifies a name for the external NTP or SNTP server.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

IP address

Specifies the IP address of the external NTP or 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 external NTP or SNTP server listens for requests.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `123`)

Status

Displays the connection status between the device and the external NTP or SNTP server.

Possible values:

- *`success`*
  The device has successfully synchronized the local system clock with the external NTP or SNTP server.
- *`badDateEncoded`*
  Synchronization was unsuccessful. The time information received contains protocol errors.
- *`other`*
  Synchronization was unsuccessful.
  - The IP address `0.0.0.0` is specified for the external NTP or SNTP server.
    or
  - The device is using a different external NTP or SNTP server.
- *`requestTimedOut`*
  Synchronization was unsuccessful. The device has not received a response from the external NTP or SNTP server.
- *`serverKissOfDeath`*
  Synchronization was unsuccessful. The external NTP or SNTP server is overloaded. The device is requested to synchronize its system clock with another NTP or SNTP server. When no other NTP or SNTP server is available, the device checks at intervals longer than the value in the *Request interval [s]* field, if the server is still overloaded.
- *`serverUnsychronized`*
  Synchronization was unsuccessful. The external NTP or SNTP server is not in sync with a reference time source.
- *`versionNotSupported`*
  Synchronization was unsuccessful. The SNTP versions of the client and server are incompatible.

Active

Activates/deactivates the connection to the external NTP or SNTP server.

Possible values:

- `marked`
  The connection to the external NTP or SNTP server is activated.
  The device has the option to access to the server.
- `unmarked` (default setting)
  The connection to the external NTP or SNTP server is deactivated.
  The device does not have the option to access to the server.

2.3.2 SNTP Server

[Time > SNTP > Server]

In this dialog, you specify the settings with which the device operates as an SNTP server. As the SNTP server, the device makes the time information available to other devices in the network. The device provides the Universal Time Coordinated (UTC) without considering local time differences.

If set accordingly, the SNTP server on the device operates in Broadcast mode. In Broadcast mode, the device makes the time information available to other devices in the network by sending Broadcasts or Multicasts.

Operation

Operation

Enables/disables the *Server* function in the device. Note the setting in the *Disable server at local time source* checkbox in the *Configuration* frame.

Possible values:

- *On*
  The *Server* function is enabled.
  The device operates as an *SNTP* server.
- *Off* (default setting)
  The *Server* function is disabled.

State

State

Displays the state of the *Server* function on the device.

Possible values:

- *disabled*
  The SNTP server is not operating.
- *notSynchronized*
  The SNTP server is operating.
  The local system clock is not in sync with a reference time source.
- *syncToLocal*
  The SNTP server is operating.
  The local system clock is in sync with the hardware clock of the device.
- *syncToRefclock*
  The SNTP server is operating.
  The local system clock is in sync with an external reference time source, like a PTP clock.
- *syncToRemoteServer*
  The SNTP server is operating.
  The local system clock is in sync with an external NTP or SNTP server which is superordinate to the device in a cascade.

Configuration

UDP port

Specifies the UDP port on which the device listens for requests.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `123`)

Broadcast admin mode

Activates/deactivates the Broadcast mode.

Possible values:

- `marked`
  The device sends SNTP packets as Broadcasts or Multicasts.
  The device also responds to SNTP requests in unicast mode.
- `unmarked` (default setting)
  The device responds to SNTP requests in unicast mode, but sends no Broadcast packets on its own.

Broadcast destination address

Specifies the destination IP address to which 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 UDP port on which the device sends the SNTP packets in Broadcast mode.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `123`)

Broadcast VLAN ID

Specifies the VLAN to which the device sends the SNTP packets in Broadcast mode.

Possible values:

- `0`
  The device sends the SNTP packets in the same VLAN in which the device management access occurs. See the *Basic Settings > Network > Global* dialog.
- `1..4042` (default setting: `1`)

Broadcast send interval [s]

Specifies the interval in seconds at which the device broadcasts SNTP packets.

Possible values:

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

Disable server at local time source

Activates/deactivates the automatic disabling of the *SNTP Server* function if the local system clock is not in sync with another external time reference.

Possible values:

- `marked`
  The automatic disabling of the *SNTP Server* function is active.
  If the device has synchronized its local system clock to an external time reference, like a PTP clock, then it keeps the *SNTP Server* function enabled. Otherwise, the device disables the *SNTP Server* function.
- `unmarked` (default setting)
  The automatic disabling of the *SNTP Server* function is inactive.
  The device keeps the *SNTP Server* function enabled, regardless of whether it has synchronized its local system clock to an external time reference.
  If the local system clock is not in sync with an external time reference, then in the SNTP packet, the device informs the client that its system clock is synchronized locally.

2.4 PTP

[Time > PTP]

The menu contains the following dialogs:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.4.1 PTP Global

[Time > PTP > Global]

In this dialog, you specify basic settings for the *PTP* function.

The Precision Time Protocol (PTP) is a procedure defined in IEEE 1588-2008 that supplies the devices in the network with a precise time. The method synchronizes the clocks in the network with a precision of a few 100 ns. The protocol uses Multicast communication, so the load on the network due to the *PTP* synchronization messages is negligible.

PTP is significantly more accurate than SNTP. If the *SNTP* function and the *PTP* function are enabled in the device at the same time, then the *PTP* function has priority.

With the *Best Master Clock* algorithm, the devices in the network determine which device has the most accurate time. The devices use the device with the most accurate time as the reference time source (*Grandmaster*). Subsequently the participating devices synchronize themselves with this reference time source.

If you want to transport PTP time accurately through the network, then use only devices with PTP hardware support on the transport paths.

The protocol differentiates between the following clocks:

- *Boundary Clock (BC)*
  This clock has any number of PTP ports and operates as both *PTP* master and *PTP* slave. In its respective network segment, the clock operates as an Ordinary Clock.
  - As *PTP* slave, the clock synchronizes itself with a *PTP* master that is higher than the device in the cascade.
  - As *PTP* master, the clock forwards the time information through the network to *PTP* slaves that are higher than the device in the cascade.
- *Transparent Clock (TC)*
  This clock has any number of PTP ports. In contrast to the *Boundary Clock*, this clock corrects the time information before forwarding it, without synchronizing itself.

Operation IEEE1588/PTP

Operation IEEE1588/PTP

Enables/disables the *PTP* function.

Possible values:

- *On*
  The *PTP* function is enabled.
  The device synchronizes its clock with PTP.
  If the *SNTP* function and the *PTP* function are enabled in the device at the same time, then the *PTP* function has priority.
- *Off* (default setting)
  The *PTP* function is disabled.
  The device transmits the *PTP* synchronization messages without any correction on every port.

Configuration IEEE1588/PTP

PTP mode

Specifies the PTP version and mode of the local clock.

Possible values:

- *v2-transparent-clock* (default setting)
- *v2-boundary-clock*

Min. acceptable sync offset [ns]

Specifies the lower threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference falls below this value once, then the device considers its local clock to be synchronized.

Possible values:

- `1..999999999 (10⁹-1)` (default setting: `30`)

Max. acceptable sync offset [ns]

Specifies the upper threshold value in nanoseconds for the path difference between the local clock and the reference time source (*Grandmaster*). If the path difference exceeds this value once, then the device considers its local clock to be unsynchronized.

Possible values:

- `31..1000000000 (10⁹)` (default setting: `5000`)

PTP management

Activates/deactivates the PTP management defined in the PTP standard.

Possible values:

- `marked`
  PTP management is activated.
- `unmarked` (default setting)
  PTP management is deactivated.

Status

Is synchronized

Displays if the local system clock is synchronized with the reference time source (*Grandmaster*).

If the path difference between the local clock and the reference time source (*Grandmaster*) falls below the synchronization lower threshold value one time, then the device considers its local clock to be synchronized. The device keeps this status until the path difference exceeds the synchronization upper threshold value one time.

You specify the synchronization threshold values in the *Configuration IEEE1588/PTP* frame.

Max. offset absolute [ns]

Displays the maximum path difference in nanoseconds that has occurred since the local system clock was synchronized with the reference time source (*Grandmaster*).

PTP time

Displays the date and time for the PTP time scale when the local clock is synchronized with the reference time source (*Grandmaster*). Format: `Month Day, Year  hh:mm:ss AM/PM`

2.4.2 PTP Boundary Clock

[Time > PTP > Boundary Clock]

With this menu you can set up the *Boundary Clock* mode for the local clock.

The menu contains the following dialogs:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

2.4.2.1 PTP Boundary Clock Global

[Time > PTP > Boundary Clock > Global]

In this dialog, you specify general, cross-port settings for the *Boundary Clock* mode for the local clock. The *Boundary Clock (BC)* operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the *Boundary Clock (BC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-boundary-clock`.

Operation IEEE1588/PTPv2 BC

Priority 1

Specifies the *priority 1* value for the device.

Possible values:

- `0..255` (default setting: `128`)

The *Best Master Clock* algorithm first evaluates the *priority 1* value among the participating devices to determine the reference time source (*Grandmaster*).

The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the *Grandmaster* frame.

Priority 2

Specifies the *priority 2* value for the device.

Possible values:

- `0..255` (default setting: `128`)

When the previously evaluated criteria are the same for multiple devices, the *Best Master Clock* algorithm evaluates the *priority 2* value of the participating devices.

The lower you set this value, the more probable it is that the device becomes the reference time source (*Grandmaster*). See the *Grandmaster* frame.

Domain number

Assigns the device to a *PTP* domain.

Possible values:

- `0..255` (default setting: `0`)

The device transmits time information from and to devices only in the same domain.

Status IEEE1588/PTPv2 BC

Two step

Displays that the clock is operating in Two-Step mode.

Steps removed

Displays the number of communication paths passed through between the local clock of the device and the reference time source (*Grandmaster*).

For a *PTP* slave, the value 1 means that the clock is connected with the reference time source (*Grandmaster*) directly through one communication path.

Offset to master [ns]

Displays the measured difference (offset) between the local clock and the reference time source (*Grandmaster*) in nanoseconds. The *PTP* slave calculates the difference from the time information received.

In Two-Step mode the time information consists of 2 *PTP* synchronization messages each, which the *PTP* master sends cyclically:

- The first synchronization message (sync message) contains an estimated value for the exact sending time of the message.
- The second synchronization message (follow-up message) contains the exact sending time of the first message.

The *PTP* slave uses the two *PTP* synchronization messages to calculate the difference (offset) from the master and corrects its clock by this difference. Here the *PTP* slave also considers the *Delay to master [ns]* value.

Delay to master [ns]

Displays the delay when transmitting the *PTP* synchronization messages from the *PTP* master to the *PTP* slave in nanoseconds.

The *PTP* slave sends a “Delay Request” packet to the *PTP* master and thus determines the exact sending time of the packet. When it receives the packet, the *PTP* master generates a time stamp and sends this in a “Delay Response” packet back to the *PTP* slave. The *PTP* slave uses the two packets to calculate the delay, and considers this starting from the next offset measurement.

The prerequisite is that in the *Time > PTP > Boundary Clock > Port* dialog, *Delay mechanism* column, the value *e2e* is specified for the slave ports.

Grandmaster

This frame displays the criteria that the *Best Master Clock* algorithm uses when evaluating the reference time source (*Grandmaster*).

The algorithm first evaluates *priority 1* of the participating devices. The device with the numerically lowest value for *priority 1* is designated as the reference time source (*Grandmaster*). When the value is the same for multiple devices, the algorithm takes the next criterion, and when this is also the same, the algorithm takes the next criterion after this one. When every value is the same for multiple devices, the numerically lowest value in the *Clock identity* field decides which device is designated as the reference time source (*Grandmaster*).

The device lets you influence which device in the network is designated as the reference time source (*Grandmaster*). To do this, modify the value in the *Priority 1* field or the *Priority 2* field in the *Operation IEEE1588/PTPv2 BC* frame.

Priority 1

Displays the *priority 1* value for the device that is currently the reference time source (*Grandmaster*).

Clock class

Displays the class of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock* algorithm.

Clock accuracy

Displays the estimated accuracy of the reference time source (*Grandmaster*). Parameter for the *Best Master Clock* algorithm.

Clock variance

Displays the variance of the reference time source (*Grandmaster*), also known as the *Offset scaled log variance*. Parameter for the *Best Master Clock* algorithm.

Priority 2

Displays the *priority 2* value for the device that is currently the reference time source (*Grandmaster*).

Local time properties

Time source

Specifies the time source from which the local clock gets its time information.

Possible values:

- *atomicClock*
- *gps*
- *terrestrialRadio*
- *ptp*
- *ntp*
- *handSet*
- *other*
- *internalOscillator* (default setting)

UTC offset [s]

Specifies the difference between the *PTP* time scale and the Universal Time Coordinated (UTC).

See the *PTP timescale* checkbox.

Possible values:

- `-32768..32767 (2¹⁵-1)`

Note:
The default setting is the value valid on the creation date of the device software. For further information, see the "Bulletin C" of the Earth Rotation and Reference Systems Service (IERS): https://www.iers.org/iers/en/dataproducts/earthorientationdata/eop

UTC offset valid

Specifies if the value specified in the *UTC offset [s]* field is correct.

Possible values:

- `marked`
- `unmarked` (default setting)

Time traceable

Displays if the reference time source (*Grandmaster*) obtains the time and date from a primary reference, for example from an NTP server.

Possible values:

- `marked`
  The device displays the exact time and date, as these are derived from a reference time source (*Grandmaster*).
- `unmarked`
  The device displays a time and date that are not derived from a reference time source (*Grandmaster*).

Frequency traceable

Displays if the reference time source (*Grandmaster*) obtains the clock frequency from a primary reference, for example from an NTP server.

Possible values:

- `marked`
  The device clock rate is synchronized with a reference rate source. Therefore, the device runs its clock at the correct and steady rate, even if the exact absolute time is not required.
- `unmarked`
  The device clock rate is not synchronized with a reference rate source.

PTP timescale

Displays if the device uses the PTP time scale.

Possible values:

- `marked`
- `unmarked`

According to IEEE 1588, the PTP time scale is the TAI atomic time started on 01.01.1970.

In contrast to Universal Time Coordinated (UTC), TAI does not use leap seconds.

As of January 6, 2026, the TAI time is 37 s ahead of the Universal Time Coordinated (UTC).

Identities

The device displays the identities as byte sequences in hexadecimal notation.

The identification numbers (UUID) are made up as follows:
- The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.
- The port UUID consists of the device identification number followed by a 16-bit port ID.

Clock identity

Displays the identification number (UUID) of the device.

Parent port identity

Displays the port identification number (UUID) of the directly superior master device.

Grandmaster identity

Displays the identification number (UUID) of the reference time source (*Grandmaster*) device.

2.4.2.2 PTP Boundary Clock Port

[Time > PTP > Boundary Clock > Port]

In this dialog, you specify the *Boundary Clock (BC)* settings on each individual port.

The settings are effective when the local clock operates as the *Boundary Clock (BC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-boundary-clock`.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

The *PTP* function is available on the following ports:
- Slot 5: ports *5/1*..*5/32*
- Slot 6: ports *6/1*..*6/4*

Port

Displays the port number.

PTP enable

Activates/deactivates transmitting *PTP* synchronization messages on the port.

Possible values:

- `marked` (default setting)
  The transmission is activated. The port forwards and receives *PTP* synchronization messages.
- `unmarked`
  The transmission is deactivated. The port blocks *PTP* synchronization messages.

PTP status

Displays the current status of the port.

Possible values:

- *`initializing`*
  Initialization phase
- *`faulty`*
  Faulty mode: error in the Precision Time Protocol (PTP).
- *`disabled`*
  PTP is disabled on the port.
- *`listening`*
  The port is waiting for *PTP* synchronization messages.
- *`pre-master`*
  PTP pre-master mode
- *`master`*
  PTP master mode
- *`passive`*
  PTP passive mode

- *uncalibrated*
  PTP uncalibrated mode
- *slave*
  PTP slave mode

Network protocol

Specifies which protocol the port uses to transmit the *PTP* synchronization messages.

Possible values:

- *802.3* (default setting)
- *UDP/IPv4*

Announce interval [s]

Specifies the interval in seconds at which the port transmits messages for the PTP topology discovery.

Assign the same value to every device of a *PTP* domain.

Possible values:

- 1
- 2 (default setting)
- 4
- 8
- 16

Announce timeout

Specifies the number of announce intervals.

Example:

For the default setting (*Announce interval [s]* = 2 and *Announce timeout* = 3), the timeout is 3 × 2 s = 6 s.

Possible values:

- 2..10 (default setting: 3)
  Assign the same value to every device of a *PTP* domain.

Sync interval [s]

Specifies the interval in seconds at which the port transmits *PTP* synchronization messages.

Possible values:

- 0.25
- 0.5
- 1 (default setting)
- 2

Delay mechanism

Specifies the mechanism with which the device measures the delay for transmitting the *PTP* synchronization messages.

Possible values:

- *disabled*
  The measurement of the delay for the *PTP* synchronization messages for the connected PTP devices is inactive.
- *e2e* (default setting)
  End-to-End: As the *PTP* slave, the port measures the delay for the *PTP* synchronization messages to the *PTP* master.
  The device displays the measured value in the *Time > PTP > Boundary Clock > Global* dialog.
- *p2p*
  Peer-to-Peer: The device measures the delay for the *PTP* synchronization messages for the connected PTP devices, provided that these devices support P2P.
  This mechanism spares the device from having to determine the delay again in the case of a reconfiguration.

P2P delay

Displays the measured Peer-to-Peer delay for the *PTP* synchronization messages.

The prerequisite is that in the *Delay mechanism* column the value *p2p* is specified.

P2P delay interval [s]

Specifies the interval in seconds at which the port measures the Peer-to-Peer delay.

The prerequisite is that in the *Delay mechanism* column the value *p2p* is specified for this port and for the port of the remote device.

Possible values:

- 1 (default setting)
- 2
- 4
- 8
- 16
- 32

E2E delay interval [s]

Displays the interval in seconds at which the port measures the End-to-End delay.

Possible values:

- When the port is operating as the *PTP* master, the device assigns to the port the value 8.
- When the port is operating as the *PTP* slave, the value is specified by the *PTP* master connected to the port.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

- `-2000000000..2000000000` (default setting: `0`)

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of y × 2 ns.

The value is positive if the delay from the *PTP* master to the *PTP* slave is longer than in the opposite direction.

VLAN

Specifies the VLAN ID that the device uses to tag the received *PTP* synchronization messages on this port.

Possible values:

- *none* (default setting)
  The device transmits *PTP* synchronization messages without a VLAN tag.
- `0..4042`
  You specify VLANs that you have already set up in the device from the list.

Verify that the port is a member of the VLAN.

See the *Switching > VLAN > Configuration* dialog.

VLAN priority

Specifies the priority with which the device transmits the *PTP* synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1D).

Possible values:

- `0..7` (default setting: `6`)

If you specified in the *VLAN* column the value *none*, then the device ignores the VLAN priority.

2.4.3 PTP Transparent Clock

[Time > PTP > Transparent Clock]

With this menu you can set up the *Transparent Clock* mode for the local clock.

The menu contains the following dialogs:

- PTP Transparent Clock Global
- PTP Transparent Clock Port

2.4.3.1 PTP Transparent Clock Global

[Time > PTP > Transparent Clock > Global]

In this dialog, you specify general, cross-port settings for the *Transparent Clock* mode for the local clock. The *Transparent Clock (TC)* operates according to PTP version 2 (IEEE 1588-2008).

The settings are effective when the local clock operates as the *Transparent Clock (TC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-transparent-clock`.

Operation IEEE1588/PTPv2 TC

Delay mechanism

Specifies the mechanism with which the device measures the delay for transmitting the *PTP* synchronization messages.

Possible values:

- `e2e` (default setting)
  As the *PTP* slave, the port measures the delay for the *PTP* synchronization messages to the *PTP* master.
  The device displays the measured value in the *Time > PTP > Transparent Clock > Global* dialog.
- `p2p`
  The device measures the delay for the *PTP* synchronization messages for every connected PTP device, provided that the device supports P2P.
  This mechanism spares the device from having to determine the delay again in the case of a reconfiguration.
  If you specify this value, then the value `802.3` is only available in the *Network protocol* column.
- `e2e-optimized`
  Like `e2e`, with the following special characteristics:
  - The device transmits the delay requests of the *PTP* slaves only to the *PTP* master, even though these requests are multicast messages. The device thus spares the other devices from unnecessary multicast requests.
  - If the master-slave topology changes, then the device relearns the port for the *PTP* master as soon as it receives a synchronization message from another *PTP* master.
  - If the device does not know a *PTP* master, then the device transmits delay requests to the ports.
- `disabled`
  The delay measuring is disabled on the port. The device discards messages for the delay measuring.

Primary domain

Assigns the device to a *PTP* domain.

Possible values:

- `0..255` (default setting: `0`)

The device transmits time information from and to devices only in the same domain.

Network protocol

Specifies which protocol the port uses to transmit the *PTP* synchronization messages.

Possible values:

- `ieee8023` (default setting)
- `udpIpv4`

Multi domain mode

Activates/deactivates the *PTP* synchronization message correction in every *PTP* domain.

Possible values:

- `marked`
  The device corrects *PTP* synchronization messages in every *PTP* domain.
- `unmarked` (default setting)
  The device corrects *PTP* synchronization messages only in the primary *PTP* domain. See the *Primary domain* field.

VLAN ID

Specifies the VLAN ID with which the device marks the *PTP* synchronization messages on this port.

Possible values:

- `none` (default setting)
  The device transmits *PTP* synchronization messages without a VLAN tag.
- `0..4042`
  You specify VLANs that you have already set up in the device from the list.

VLAN priority

Specifies the priority with which the device transmits the *PTP* synchronization messages marked with a VLAN ID (Layer 2, IEEE 802.1D).

Possible values:

- `0..7` (default setting: `6`)

If you specified the value `none` in the *VLAN ID* field, then the device ignores the specified value.

Local synchronization

Syntonize

Activates/deactivates the frequency synchronization of the *Transparent Clock* with the *PTP* master.

Possible values:

- `marked` (default setting)
  The frequency synchronization is active.
  The device synchronizes the frequency.
- `unmarked`
  The frequency synchronization is inactive.
  The frequency remains constant.

Synchronize local clock

Activates/deactivates the synchronization of the local system time.

Possible values:

- `marked`
  The synchronization is active.
  The device synchronizes the local system time with the time received using PTP. The prerequisite is that the *Syntonize* checkbox is marked.
- `unmarked` (default setting)
  The synchronization is inactive.
  The local system time remains constant.

Current master

Displays the port identification number (UUID) of the directly superior master device on which the device synchronizes its frequency.

If the value contains only zeros, this is because:

- The *Syntonize* function is disabled.
  or
- The device cannot find a *PTP* master.

Offset to master [ns]

Displays the measured difference (offset) between the local clock and the *PTP* master in nanoseconds. The device calculates the difference from the time information received.

The prerequisite is that the *Synchronize local clock* function is enabled.

Delay to master [ns]

Displays the delay when transmitting the *PTP* synchronization messages from the *PTP* master to the *PTP* slave in nanoseconds.

Prerequisites:

- The *Synchronize local clock* function is enabled.
- In the *Delay mechanism* field, the value `e2e` is selected.

Status IEEE1588/PTPv2 TC

Clock identity

Displays the identification number (UUID) of the device.

The device displays the identities as byte sequences in hexadecimal notation.

The device identification number consists of the MAC address of the device, with the values `ff` and `fe` added between byte 3 and byte 4.

2.4.3.2 PTP Transparent Clock Port

[Time > PTP > Transparent Clock > Port]

In this dialog, you specify the *Transparent Clock (TC)* settings on each individual port.

The settings are effective when the local clock operates as the *Transparent Clock (TC)*. For this, you select in the *Time > PTP > Global* dialog in the *PTP mode* field the value `v2-transparent-clock`.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

PTP enable

Activates/deactivates transmitting *PTP* synchronization messages on the port.

Possible values:

- `marked` (default setting)
  The transmitting is active.
  The port forwards and receives *PTP* synchronization messages.
- `unmarked`
  The transmitting is inactive.
  The port blocks *PTP* synchronization messages.

P2P delay interval [s]

Specifies the interval in seconds at which the port measures the Peer-to-Peer delay.

The prerequisite is that in the *Time > PTP > Transparent Clock > Global* dialog, *Delay mechanism* option list, the radio button `p2p` is selected for this port and for the port of the remote device.

Possible values:

- `1` (default setting)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P delay

Displays the measured Peer-to-Peer delay for the *PTP* synchronization messages.

The prerequisite is that in the *Time > PTP > Transparent Clock > Global* dialog, *Delay mechanism* option list, the radio button `p2p` is selected.

Asymmetry

Corrects the measured delay value corrupted by asymmetrical transmission paths.

Possible values:

- `-2000000000..2000000000 (2× 10⁹)` (default setting: `0`)

The value represents the delay symmetry in nanoseconds.

A measured delay value of y ns corresponds to an asymmetry of y × 2 ns.

The value is positive if the delay from the *PTP* master to the *PTP* slave is longer than in the opposite direction.

3 Device Security

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

3.1 User Management

[Device Security > User Management]

If users log into the device management 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
- Password policy settings 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 possible consecutive unsuccessful login attempts when the user accesses the device management using the Graphical User Interface or the Command Line Interface.

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

Possible values:

▶ `0..5` (default setting: `0`)

If the user makes one more consecutive 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 into the device management.

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`)

Auto-unlock users

Activates/deactivates the automatic unlocking of user accounts the device has locked due to the specified number of consecutive failed login attempts. See the *Login attempts* field in the *Configuration* frame.

Possible values:

- `marked`
  The user account unlocking is active. The device unlocks a locked user account after the period specified in the *Auto-unlock timer [min]* column.
- `unmarked` (default setting)
  The user account unlocking is inactive. A locked user account remains locked until an administrator unlocks it.

Password policy

This frame lets you specify the policy for valid passwords. The device uses this policy to check a new or changed password, provided the password policy check is enabled for the respective password.

The settings affect the passwords in the *Password* column, if the corresponding 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.

Note:
Permitted special characters are: `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

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 18.

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 add a user account, click the button.

Active

Activates/deactivates the user account.

Possible values:

- `marked`
  The user account is active. The device accepts the login of a user, to the device management, with this user name.
- `unmarked` (default setting)
  The user account is inactive. The device rejects the login of a user, to the device management, with this user name.

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

Password

Specifies the password that the user applies to access the device management using the Graphical User Interface or Command Line Interface. The device displays ●●●●● (dots) instead of the password.

To change the *Password* value, click the relevant field. The device opens a password entry/change dialog, see “Password entry/change dialog” on page 115.

When you specify the password for the first time, the device uses the same password also 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 you did not individually specify them previously.

Possible values:

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

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. For that, the device uses a password change/entry dialog, see “Password entry/change dialog” on page 115.

The device always checks the minimum length of the password, even if the checkbox in the *Policy check* column is `unmarked`. You specify the required minimum length of the password in the *Configuration* frame.

Role

Specifies the access role that controls 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 to the device management.
  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 consecutive 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.

Auto-unlock timer [min]

Specifies the time in minutes after which the device unlocks a locked user account. This setting is effective only if the *Auto-unlock users* checkbox is marked in the *Configuration* frame.

The timer starts when the device locks the account due to the specified number of consecutive failed login attempts. See the *Login attempts* field in the *Configuration* frame.

Possible values:

- `1..720` (default setting: `30`)

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.

Note:
The device always checks the minimum length of the password, even if the checkbox in the *Policy check* column is `unmarked`.

SNMP auth type

Specifies the algorithm that the device uses to authenticate the selected SNMPv3 user.

Possible values:

- *hmacmd5* (default setting)
  MD5
- *hmacsha*
  SHA-1
- *hmacsha256*
  SHA-256

SNMP auth password

Specifies the password that the device applies for user access using SNMPv3. The device displays ●●●●● (dots) instead of the password.

To change the *SNMP auth password* value, click the relevant field. The device opens a password entry/change dialog, see “Password entry/change dialog” on page 115.

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 algorithm that the device uses to encrypt SNMPv3 messages for the selected SNMPv3 user.

Possible values:

- *none*
  No encryption.
- *des* (default setting)
  DES
- *aesCfb128*
  AES-128
- *aesCfb256*
  AES-256

SNMP encryption password

Specifies the password that the device applies to encrypt user access using SNMPv3. The device displays ●●●●● (dots) instead of the password.

To change the *SNMP encryption password* value, click the relevant field. The device opens a password entry/change dialog, see "Password entry/change dialog" on page 115.

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
  - !#$%&'()*+,-./:;<=>?@[\]^_`{}~

Password entry/change dialog

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
  - This check is always active.
- The dialog checks if the entered password matches the password policy.
  - This check is active only if you activated the *Policy check* checkbox for the respective password field.
- The dialog checks if the entered password contains only allowed characters.
  - This check is always active.
- The dialog helps avoid typos in the password by having you enter the password twice.
  - This check is always active.

Password length (min.):

This dialog element displays the required minimum length of the password.

- If the currently entered password satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
This check is always active.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
This check is always active.

Upper-case characters (min.):

This dialog element displays the required minimum number of uppercase characters in the password.

- If the password satisfies the required min. number of uppercase characters:
  - The device displays a green checkmark to the left of the text *Upper-case characters (min.):*
  - The device displays the text *Upper-case characters (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
This check is active only if you activated the *Policy check* checkbox for the respective password field.

Lower-case characters (min.):

This dialog element displays the required minimum number of lowercase characters in the password.

- If the password satisfies the required min. number of lowercase characters:
  - The device displays a green checkmark to the left of the text *Lower-case characters (min.):*
  - The device displays the text *Lower-case characters (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
This check is active only if you activated the *Policy check* checkbox for the respective password field.

Digits (min.):

This dialog element displays the required minimum number of digits in the password.

- If the password satisfies the required min. number of digits:
  - The device displays a green checkmark to the left of the text *Digits (min.):*
  - The device displays the text *Digits (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
This check is active only if you activated the *Policy check* checkbox for the respective password field.

Special characters (min.):

This dialog element displays the required minimum number of special characters in the password.

- If the password satisfies the required min. number of special characters:
  - The device displays a green checkmark to the left of the text *Special characters (min.):*
  - The device displays the text *Special characters (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Note:
Permitted special characters are: `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`
This check is active only if you activated the *Policy check* checkbox for the respective password field.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

3.2 Authentication List

[Device Security > 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 18.

Note:
If the table does not contain a list, then access to the device management is only possible using the Command Line Interface through the serial connection. In this case, the device authenticates the user 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 item 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 item 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 add a 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.
- *reject*
  The device accepts or rejects the user logging into the device management 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 into the device management without attempting the other polices.
  - 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 into the device management using the other polices 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 > IAS* 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

[Device Security > 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 Lightweight Directory Access Protocol (LDAP). 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 caches the login data. This speeds up the login process when users log into the device management 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

[Device Security > 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

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 into the device management through LDAP.

Possible values:

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

Configuration

Buttons

Flush cache

Deletes the cached login data of the successfully logged in users.

Client cache timeout [min]

Specifies for how many minutes after successfully logging into the device management 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 into 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 attempts to authenticate on the LDAP server with the user ID to find the “Distinguished Name” (DN) for the users logging into the device management. 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 into the LDAP server. The device displays ●●●●● (dots) instead of the password.

To change the *Bind user password* value, click the relevant field. The device opens a password entry/change dialog, see “Password entry/change dialog” on page 124.

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 into the device management.

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

Password entry/change dialog

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (min.):

This dialog element displays the required minimum length of the password.

- If the currently entered password satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

Certificates/CRLs

To establish a secure connection, the device requires to obtain a valid digital certificate to verify the identity of the server. The prerequisite is that you have transferred the public certificate of the server onto the device. Ask the server administrator for a digital certificate in X.509 format. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

A Certificate Revocation List (CRL) contains a list of digital certificates revoked by the Certification Authority (CA) before their scheduled expiration date. When establishing a secure connection to the server, the device stops setting up the connection if the CRL includes the public certificate of the server. The device logs the event in the System Log. For security reasons, Hirschmann recommends using only CRLs signed by a Certification Authority (CA).

Buttons

Clear all Certificates/CRLs

Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (*NVM*).

URL

Specifies the path and file name of the digital certificate or CRL.

The device accepts digital certificates and CRLs with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines
  ```
  -----BEGIN CERTIFICATE-----
  …
  -----END CERTIFICATE-----
  ```
  or
  ```
  -----BEGIN CRL-----
  …
  -----END CRL-----
  ```

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  When the file 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 through TFTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Transfers the file specified in the *URL* field onto the device.

In this dialog, you can transfer a maximum of 16 digital certificates and additionally a maximum of 16 CRLs onto the device.

For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the *LDAP* function. See the *Operation* frame.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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.

If in the *Connection security* column a value other than *none* is specified and the digital certificate contains only DNS names of the server, then specify a DNS name.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)
- Valid IPv6 address
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
  The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.
- `_ldap._tcp.<domain>.<tld>`
  Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.

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 (2¹⁶-1)` (default setting: `389`)

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 digital certificate contains only the DNS names, then specify the DNS name of the server in the *Address* column. Enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.

If the digital 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 setting.

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 digital 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

[Device Security > LDAP > Role Mapping]

This dialog lets you set 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 into the device management, 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 18.

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

3.4 Management Access

[Device Security > Management Access]

The menu contains the following dialogs:

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

3.4.1 Server

[Device Security > Management Access > 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 18.

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 (SSH). 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`
  SNMP version 1 access is active.
  - You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
  - You activate/deactivate the write access for the *read and write* authorization in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
- `unmarked` (default setting)
  SNMP version 1 access is inactive.

SNMPv2

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

Possible values:

- `marked`
  SNMP version 2 access is active.
  - You specify the community names in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
  - You activate/deactivate the write access for the *read and write* authorization in the *Device Security > Management Access > SNMPv1/v2 Community* dialog.
- `unmarked` (default setting)
  SNMP version 2 access is inactive.

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 (2¹⁶-1)` (default setting: `161`)

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.

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

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

Configuration

TCP port

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

Possible values:

- `1..65535 (2¹⁶-1)` (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 into the device management.

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

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 generate the RSA *host key* directly in the device. As an alternative, you can transfer your own private RSA key in PEM format onto the device.

Furthermore, the device can load an RSA *Host Key*, which is stored on the external memory (*ENVM*), during 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 access to the device management is only possible using the Command Line Interface through the serial connection.

Configuration

TCP port

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

Possible values:

- `1..65535 (2¹⁶-1)` (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 into the device management has been inactive for this time, the device ends the connection.

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

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`
  The RSA *host key* is present.
- `unmarked`
  The RSA *host key* is not present.

Create

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

Length of the key generated:

- 2048 bit (RSA)

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

As an alternative, you can transfer your own private RSA key in PEM format onto the device. See the *Key import* frame.

Delete

Deletes the RSA *host key* from the device. The prerequisite is that the SSH server is disabled.

Oper status

Displays if the device currently generates a RSA *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 an RSA *host key*.

Fingerprint

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

After importing a new RSA *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 SHA-256 hash.

RSA fingerprint

Displays the fingerprint of the RSA *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 private RSA key.

The device accepts the key if it has a length of 2048, 3072, or 4096 bits.

The device gives you the following options for transferring the file onto the device:

- Import from the PC
  When the file is located on your PC or on a network drive, drag and drop it onto the ⬆ area.
  As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on an FTP server, specify the URL for the file in the following form:
  `ftp://<user>:<password>@<IP address>[:port]/<file name>`

- Import through TFTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  – `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Transfers the file specified in the *URL* field onto the device.

For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the *SSH server* function. See the *Operation* frame.

[HTTP]

This tab lets you enable/disable the Hypertext Transfer Protocol (HTTP) 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 Hypertext Transfer Protocol (HTTP) and use the Hypertext Transfer Protocol Secure (HTTPS) 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* function for the web server.

Possible values:

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

Note:
If the *HTTP* and *HTTPS* functions are disabled, then you can enable the *HTTP* function 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 (2¹⁶-1)` (default setting: `80`)
  Exception: Port `2222` is reserved for internal functions.

[HTTPS]

This tab lets you enable/disable the Hypertext Transfer Protocol Secure(HTTPS) 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 generate this digital certificate yourself or to transfer an existing digital 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* function for the web server.

Possible values:

- *On* (default setting)
  The *HTTPS* function 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* function.
- *Off*
  The *HTTPS* function is disabled.
  When the *HTTP* function is enabled, the access to the device management is possible through an unencrypted *HTTP* connection.

Note:
If the *HTTP* and *HTTPS* functions are disabled, then you can enable the *HTTPS* function 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 (2¹⁶-1)` (default setting: `443`)
  Exception: Port `2222` is reserved for internal functions.

Certificate

If the device uses a digital 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:

- Transfer a digital certificate onto the device whose Certification Authority (CA) is known to your web browser. This may additionally require you to make the Certification Authority (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 a digital certificate is present in the device.

Possible values:

- `marked`
  A digital certificate is present.
- `unmarked`
  The digital 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 digital certificate, restart the web server. Restarting the web server is possible only through the Command Line Interface.

You can transfer a digital certificate onto 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 digital certificate.
- *delete*
  The device currently deletes a digital certificate.
- *generate*
  The device currently generates a digital 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 SHA-1 fingerprint of the digital certificate.
- `sha256` (default setting)
  The *Fingerprint* field displays the SHA-256 fingerprint of the digital 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 digital certificate.

The device accepts digital certificates with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines
  - `-----BEGIN PRIVATE KEY-----`
    …
    `-----END PRIVATE KEY-----`
    or
  - `-----BEGIN CERTIFICATE-----`
    …
    `-----END CERTIFICATE-----`
- RSA key with a length of 2048, 3072, or 4096 bits

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the ⬆ area. As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  When the file 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 through TFTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  When the file is on an SCP or SFTP server, specify the URL for the file in the following form:
  – `scp://` or `sftp://<IP address>[:port]/<path>/<file name>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  – `scp://` or `sftp://<user>:<password>@<IP address>[:port]/<path>/<file name>`
  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Transfers the file specified in the *URL* field onto the device.

For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the *HTTPS server* function. See the *Operation* frame.

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

This dialog lets you restrict access to the device management from a specific IP address range for selected applications.

- If the function is disabled, then access to the device management is unrestricted. Everyone can access the device management from any IP address using any application.
- If the function is enabled, then access is restricted. Everyone can access the device management only under the following conditions:
  - At least one rule is active.
    and
  - You access the device with a permitted application from a permitted IP address range specified in the rule.

Operation

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.

Note:
Before you enable the function, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.

▶ *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 18.

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 add a 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`)
  Example: To restrict access from a single IP address, specify the value as `255.255.255.255`.

HTTP

Activates/deactivates the HTTP access.

Possible values:

- `marked` (default setting)
  HTTP access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  HTTP access is inactive.

HTTPS

Activates/deactivates the HTTPS access.

Possible values:

- `marked` (default setting)
  HTTPS access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  HTTPS access is inactive.

SNMP

Activates/deactivates the SNMP access.

Possible values:

- `marked` (default setting)
  SNMP access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  SNMP access is inactive.

Telnet

Activates/deactivates the Telnet access.

Possible values:

- `marked` (default setting)
  Telnet access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  Telnet access is inactive.

SSH

Activates/deactivates the SSH access.

Possible values:

- `marked` (default setting)
  SSH access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  SSH access is inactive.

Active

Activates/deactivates the table row.

Possible values:

- `marked` (default setting)
  The table row is active. The device restricts the access to the device management from the specified IP address range for the selected applications.
- `unmarked`
  The table row is inactive. The device does not restrict access to the device management from the specified IP address range for the selected applications.

3.4.3 Web

[Device Security > Management Access > 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 into the device management.

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

[Device Security > Management Access > CLI]

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 to activate automatic closing of inactive Command Line Interface sessions through the serial connection.

You can access the device management using the Command Line Interface in the following ways:
- Through a serial connection over the V.24 interface
- Through SSH over Ethernet

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
  – `%s` short product name
  – `%t` time
Default setting: `(DRAGON)`

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 into the device management using the Command Line Interface through the serial connection.

Possible values:

▶ `0..160` (default setting: `5`)
The value `0` deactivates the function, and the user remains logged into the device management when inactive.

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

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 into the device management through 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

[Device Security > Management Access > SNMPv1/v2 Community]

In this dialog, you specify the community name for SNMPv1/v2 applications and activate/deactivate the write access for the *read and write* authorization.

Applications send requests using SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name (see *Community* column) and the write access setting (see the checkbox in the *SNMP V1/V2 readOnly* column), the application gets *read-only* authorization or *read and write* authorization.

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 18.

Community

Displays the authorization for SNMPv1/v2 access to the device.

Possible values:

- `Write`
  For requests with the community name entered, the application receives *read and write* authorization.
  If the *SNMP V1/V2 readOnly* checkbox is marked, then the application receives *read-only* authorization.
- `Read`
  For requests with the community name entered, the application receives *read-only* authorization.

Name

Specifies the community name for the adjacent authorization.

Possible values:

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

  `private` (default setting for *read and write* authorization)
  `public` (default setting for *read-only* authorization)

Configuration

SNMP V1/V2 readOnly

Activates/deactivates the write access for the `Write` community.

Possible values:

- `marked`
  The write access for the `Write` community is inactive.
  For requests with the community name entered, the application receives *read-only* authorization.
- `unmarked` (default setting)
  The write access for the `Write` community is active.
  For requests with the community name entered, the application receives *read and write* authorization.

3.5 Pre-login Banner

[Device Security > Pre-login Banner]

This dialog lets you display a greeting or information text to users before they log into the device management.

The users see this text in the login dialog of the Graphical User Interface and of the Command Line Interface. Users logging into the device management 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

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, the device saves this text.

Banner text

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>`

3.6 SSH Known Hosts

[Device Security > SSH Known Hosts]

The device permits SSH-based connections only to remote servers that are known to the device. In the state on delivery, no remote server is set up as a known host on the device.

In this dialog, you make the remote servers known by their public key fingerprints. You can set up a maximum of 50 entries containing the server address and the public key fingerprint. The device verifies the identity of the remote server by comparing the public key fingerprint stored on the device with the fingerprint calculated from the public key which the remote server actually sent. If the calculated public key fingerprint does not match the stored public key fingerprint, the device terminates the connection.

If a remote server has several keys set up, for different encryption algorithms, add each of the public key fingerprints as a separate entry.

Note:
Verify that the public key fingerprints you store on the device are from a trustworthy source, the SSH server administrator, for example.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
  Possible values:
  ▶ `1..50`
  The device lets you specify up to 50 known hosts.
- In the *Address* field, you specify the address of the server. If the server can be accessed using both an IP address and a DNS name, then add a separate table row for each address type.
  Possible values:
  – Valid IPv4 address
  – Valid IPv6 address
  – DNS hostname

- In the *Key fingerprint* field, you specify the public key fingerprint of the server.
  You can find out the public key fingerprint of the server, for example, as follows:
  – from the administrator of a known SSH server
  – from the error message following an unsuccessful software update in the *Software* dialog due to the mismatch between the public key fingerprint stored in the device and the fingerprint calculated from the public key which the remote server actually sent.
    Do not use this method if you transmit data over untrusted networks.
  Possible values:
  ▶ Base64-coded SHA-256 hash sequence with a length of 43 or 44 characters
- In the *Key type* field, you specify the algorithm that was used for generating the public key of the server. You can find out the *Key type* value simultaneously and through the same method you used to obtain the public key fingerprint.
  If you accidentally select a different algorithm, then the device cannot identify the public key using the public key fingerprint.
  Possible values:
  ▶ *dsa*
  ▶ *rsa*
  ▶ *ecdsa*
  ▶ *ed25519*



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.

Address

Displays the address of the server.

Possible values:
▶ Valid IPv4 address
▶ Valid IPv6 address
▶ DNS hostname

Key fingerprint

Specifies the public key fingerprint of the server.

Possible values:
▶ Base64-coded SHA-256 hash sequence with a length of 43 or 44 characters
  To modify the public key fingerprint, first unmark the checkbox in the *Active* column.

Key type

Displays the algorithm that was used for generating the public key of the server.

Possible values:
▶ *dsa*
▶ *rsa*

- *ecdsa*
- *ed25519*

Active

Activates/deactivates the table row.

Possible values:

- `marked` (default setting)
  The table row is active.
  The device considers the server set up in this table row to be known. When you transfer a file from an external server onto the device or vice versa, the device verifies the identity of the external server based on this public key fingerprint.
- `unmarked`
  The table row is inactive.
  The device considers the server set up in this table row to be unknown. When you transfer a file from an external server onto the device or vice versa, the device terminates the connection to this server.

4 Network Security

The menu contains the following dialogs:

- Network Security Overview
- Port Security
- 802.1X
- RADIUS
- DoS
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

4.1 Network Security Overview

[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 set-up *ACL* rules
  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.



Expands the levels. The overview then displays every level of the items.

To collapse the levels again, click the  button. The overview then displays only the first 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

[Network Security > 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

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 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.

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 18.

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 165.

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 or *HIPER Ring*, we recommend that you unmark the checkbox for the ring ports.

Note:
When you operate the device as an active participant of a *Ring/Network Coupling* or *RCP*, we recommend that you unmark the checkbox for the relevant coupling 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.

Deletes 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

Adds 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

[Network Security > 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 (IAS)

4.3.1 802.1X Global

[Network Security > 802.1X > Global]

This dialog lets you specify basic settings for the port-based access control.

Operation

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 sets up 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.

MAC authentication bypass format options

Group size

Specifies the size of the MAC address groups. The device splits the MAC address for authentication into groups. The size of the groups is specified in half bytes, each of which is represented as one character.

Possible values:

- *1*
  The device splits the MAC address into 12 groups of one character.
  Example: `A-A-B-B-C-C-D-D-E-E-F-F`
- *2*
  The device splits the MAC address into 6 groups of 2 characters.
  Example: `AA-BB-CC-DD-EE-FF`
- *4*
  The device splits the MAC address into 3 groups of 4 characters.
  Example: `AABB-CCDD-EEFF`
- *12* (default setting)
  The device formats the MAC address as one group of 12 characters.
  Example: `AABBCCDDEEFF`

Group separator

Specifies the character which separates the groups.

Possible values:

- `-` (default setting)
  dash
- *:*
  colon
- `.`
  dot

Note:
For a group size of *12*, the separator character has no effect.

Upper or lower case

Specifies if the device formats the authentication data in lowercase or uppercase letters.

Possible values:

- `lower-case`
- `upper-case` (default setting)

Password

Specifies the optional password for the clients which use the authentication bypass. The device displays ●●●●● (dots) instead of the password.

To change the *Password* value, click the relevant field. The device opens a password entry/change dialog, see "Password entry/change dialog" on page 170.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
- `<empty>`
  The device uses the client device MAC address, formatted according to the *MAC authentication bypass format options*, as both the username and the password.

Password entry/change dialog

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

Clear Password

Clears the optional password. The device then uses the client device MAC address, formatted according to the *MAC authentication bypass format options*, as both the username and the password.

Information

Monitor mode clients

Displays to 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 the protocol 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

[Network Security > 802.1X > Port Configuration]

This dialog lets you specify the access settings for every port.

When multiple end devices are connected to a port, the device lets you authenticate these individually (multi-client authentication). In this case, the device lets logged in end devices have access to the network. In contrast, the device blocks access for unauthenticated end devices, or for end devices whose authentication has elapsed.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

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.
- *multiClient*
  The device grants access to the network if the end device logs in successfully.
  If the end device does not send any EAPOL data packets, then the device grants or denies access to the network individually depending on the MAC address of the end device. See the *MAC authorized bypass* column.
  You use this setting if multiple end devices are connected to the port or if the *MAC authorized bypass* function is required.

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.

Assigned VLAN ID

Displays 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 that the authenticator assigned to the ports in the *Network Security > 802.1X > Port Clients* dialog.

For the ports in which the *Port control* column contains the value *multiClient*, the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.

Reason

Displays the reason for the assignment of the VLAN. 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 that the authenticator assigned to the ports for a supplicant in the *Network Security > 802.1X > Port Clients* dialog.

Guest VLAN ID

Specifies 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* or *multiClient*.

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.

Unauthenticated VLAN ID

Specifies 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.

MAC authorized bypass

Activates/deactivates the MAC-based authentication.

This function lets you authenticate end devices without IEEE 802.1X support on the basis of their MAC address.

Possible values:

- `marked`
  The MAC-based authentication is active.
  The device sends the MAC address of the end device to the RADIUS authentication server. The device assigns the end device to the respective VLAN based on its MAC address, as if the end device had authenticated directly using the *802.1X* protocol.
  The prerequisite is that in the *Port control* column, the *multiClient* item is selected from the drop-down list.
- `unmarked` (default setting)
  The MAC-based authentication is inactive.

MAB authentication method

Specifies the method that MAC Authentication Bypass uses on this port to authenticate the client device before granting network access.

Note:
With PAP, the device transmits the authentication credentials in plain text. CHAP and EAP-MD5 use a challenge-response mechanism instead. Use *chap* or *eap-md5* whenever possible, if the RADIUS server supports these methods.

Possible values:

- *eap-md5*
  EAP-MD5
- *pap* (default setting)
  PAP
- *chap*
  CHAP

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 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.

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 (2¹⁶-1)` (default setting: `3600`)

Users (max.)

Specifies the upper limit for the number of end devices that the device authenticates on this port at the same time. This upper limit applies only to ports in which the *Port control* column contains the value *`multiClient`*.

Possible values:

- `1..16` (default setting: `16`)

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 (2¹⁶-1)` (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 (2¹⁶-1)` (default setting: `30`)

Supplicant timeout [s]

Specifies the period in seconds for which the authenticator waits for the login of the end device.

Possible values:

- `1..65535 (2¹⁶-1)` (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 (2¹⁶-1)` (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 [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`)

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.

Status

Displays the current status of the Authenticator (`Authenticator PAE state`).

Possible values:

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

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*

Initialize port

Activates/deactivates the port initialization 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* or *multiClient*.

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.

Reauthenticate

Activates/deactivates the one-time reauthentication request.

Use this function only on ports in which the *Port control* column contains the value *auto* or *multiClient*.

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.

4.3.3 802.1X Port Clients

[Network Security > 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 18.

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.

Filter ID

Displays the name of the filter list that the RADIUS authentication server assigned to the end device after successful authentication.

The authentication server transfers the filter ID attributes in the Access Accept data packet.

Assigned VLAN ID

Displays the VLAN that the authenticator assigned to the port after the successful authentication of the end device.

If for the port in the *Network Security > 802.1X > Port Configuration* dialog, *Port control* column the value *multiClient* is specified, then the device assigns the VLAN tag based on the MAC address of the end device when receiving data packets without a VLAN tag.

VLAN 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* or *multiClient* 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

[Network Security > 802.1X > 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 18.

Buttons

Reset statistics

Resets the statistics of the selected table rows.

Port

Displays the port number.

Received

Displays the total number of EAPOL data packets that the device received on the port.

Transmitted

Displays the total number of EAPOL data packets that the device sent on the port.

Start

Displays the number of EAPOL start data packets that the device received on the port.

Logoff

Displays the number of EAPOL logoff data packets that the device received on the port.

Response/ID

Displays the number of EAP response/identity data packets that the device received on the port.

Response

Displays the number of valid EAP response data packets that the device received on the port (without EAP response/identity data packets).

Request/ID

Displays the number of EAP request/identity data packets that the device received on the port.

Request

Displays the number of valid EAP request data packets that the device received on the port (without EAP request/identity data packets).

Invalid

Displays the number of EAPOL data packets with an unknown frame type that the device received on the port.

Received error

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

[Network Security > 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 18.

Buttons

Remove

Removes the selected table row.

Port

Displays the port number.

Time

Displays the time at which the authenticator authenticated the end device.

Present for

Displays the time that has elapsed since the device generated this log entry.

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.

Status

Displays the status of the authentication on the port.

Possible values:

- *success*
  The authentication was successful.
- *failure*
  The authentication did not succeed.

Access

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.

VLAN type

Displays the type of the VLAN that the authenticator assigned to the port.

Possible values:

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Reason

Displays the reason for assigning the VLAN and the VLAN type.

4.3.6 802.1X Integrated Authentication Server (IAS)

[Network Security > 802.1X > IAS]

The Integrated Authentication Server (IAS) lets you authenticate end devices using the protocol 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 18.

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 add a user account, click the button.

Password

Specifies the password with which the user authenticates. The device displays ●●●●● (dots) instead of the password.

To change the *Password* value, click the relevant field. The device opens a password entry/change dialog, see “[Password entry/change dialog]” on page 186.

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 with this login data using the protocol 802.1X.
- `unmarked` (default setting)
  The login data is inactive.

[Password entry/change dialog]

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (min.):

This dialog element displays the required minimum length of the password.

- If the currently entered password satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

4.4 RADIUS

[Network Security > 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

[Network Security > RADIUS > Global]

This dialog lets you specify basic settings for RADIUS.

RADIUS configuration

Buttons

Reset

Deletes the statistics in the *Network Security > RADIUS > Authentication Statistics* dialog and in the *Network Security > RADIUS > Accounting Statistics* dialog.

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

[Network Security > 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 18.

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.
- In the *Secret* field, specify the shared secret. The *RADIUS* Authentication server uses this shared secret to verify that the request comes from a trusted device rather than a spoofed one. Leaving the *Secret* field empty will lead to the *RADIUS* Authentication server silently discarding each request.
  Possible values:
  ▶ Alphanumeric ASCII character string with 1..64 characters
  The device accepts the following characters:
  ```
  a..z
  A..Z
  0..9
  !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
  ```


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.

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 (2¹⁶-1)` (default setting: `1812`)

Secret

Specify a secret with which the device logs into the authentication server. The device displays ●●●●● (dots) instead of the secret.

To change the secret, click the relevant field. The device opens a secret entry/change dialog, see "[Secret entry/change dialog]" on page 193.

Possible values:

- Alphanumeric ASCII character string with 1..64 characters

You get the secret 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 authentication 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.

[Secret entry/change dialog]

If you click a Secret field, the device displays a secret entry/change dialog. The dialog lets you specify a valid secret by displaying the required secret criteria. The dialog gives you feedback on which criteria the currently entered secret meets.

- The dialog checks if the entered secret matches the required secret length.
- The dialog checks if the entered secret contains only allowed characters.
- The dialog helps avoid typos in the secret by having you enter the secret twice.

Password length (min.):

This dialog element displays the required minimum length of the secret.

- If the currently entered secret satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Password length (max.):

This dialog element displays the required maximum length of the secret.

- If the secret satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the secret contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed secret here. The device displays ●●●●● (dots) instead of the secret.

The secret entered here must match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed secret. The device displays ●●●●● (dots) instead of the secret.

The secret entered here must match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the secret to the Secret field in the underlying dialog, provided:

- The currently entered secret matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the secret in the underlying dialog unchanged.

4.4.3 RADIUS Accounting Server

[Network Security > 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 18.

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.
- In the *Secret* field, specify the shared secret. The *RADIUS* Accounting server uses this shared secret to verify that the request comes from a trusted device rather than a spoofed one. Leaving the *Secret* field empty may lead to security risks or cause the *RADIUS* Accounting server to reject packets.
  Possible values:
  ▶ Alphanumeric ASCII character string with 1..64 characters
  The device accepts the following characters:
  `a..z`
  `A..Z`
  `0..9`
  `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`



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 (2¹⁶-1)` (default setting: `1813`)

Secret

Specify a secret with which the device logs into the accounting server. The device displays ●●●●● (dots) instead of the secret.

To change the secret, click the relevant field. The device opens a secret entry/change dialog, see “[Secret entry/change dialog]” on page 193.

Possible values:

- Alphanumeric ASCII character string with 1..64 characters

You get the secret from the administrator of the accounting server.

Active

Activates/deactivates the connection to the accounting 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

[Network Security > 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 18.

Name

Displays the name of the server.

IP 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 requests

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

[Network Security > 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 18.

Name

Displays the name of the server.

IP 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 requests

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 requests

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 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

[Network Security > DoS]

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. 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

[Network Security > 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.

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 detects incoming data packets whose IP payload length in the IP header minus the outer IP header size is smaller than the minimum TCP header size. If this is the first fragment that the device detects, then the device 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
- Broadcast pings

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`)

Drop broadcast ping

Activates/deactivates the filter for Broadcast Pings. Broadcast Pings are a known evidence for Smurf Attacks.

Possible values:

- `marked`
  The filter is active.
  The device detects Broadcast Pings and drops them.
- `unmarked` (default setting)
  The filter is inactive.

4.6 DHCP Snooping

[Network Security > DHCP Snooping]

DHCP Snooping is a function that supports the network security. DHCP Snooping monitors DHCP packets between DHCP clients and the DHCP server and acts like a firewall between the untrusted hosts and the trusted DHCP servers.

In this dialog, you set up and monitor the following device behavior:
- Validate DHCP packets from untrusted sources and filter out invalid packets.
- Limit the amount of DHCP data packets from trusted and untrusted sources.
- Set up and update the DHCP Snooping binding database. This database contains the MAC address, IP address, VLAN and port of DHCP clients at untrusted ports.
- Validate follow-up requests from untrusted hosts on the basis of the DHCP Snooping binding database.

You can activate DHCP Snooping globally and for a specific VLAN. You specify the security status (trusted or untrusted) on individual ports. Verify that the DHCP service can be reached through trusted ports. For DHCP Snooping you typically set up the user/client ports as untrusted and the uplink ports as trusted.

The menu contains the following dialogs:
- DHCP Snooping Global
- DHCP Snooping Configuration

- DHCP Snooping Statistics
- DHCP Snooping Bindings

4.6.1 DHCP Snooping Global

[Network Security > DHCP Snooping > Global]

This dialog lets you set up the global DHCP Snooping parameters for your device:
- Activate/deactivate *DHCP Snooping* globally.
- Activate/deactivate *Auto-Disable* globally.
- Enable/disable the checking of the source MAC address.
- Specify the name, storage location and storing interval for the binding database.

Operation

Operation

Enables/disables the DHCP Snooping function globally.

Possible values:

- *On*
- *Off* (default setting)

Configuration

Verify MAC

Activates/deactivates the source MAC address verification in the Ethernet packet.

Possible values:

- `marked`
  The source MAC address verification is active.
  The device compares the source MAC address with the MAC address of the client in the received DHCP packet.
- `unmarked` (default setting)
  The source MAC address verification is inactive.

Auto-disable

Activates/deactivates the *Auto-Disable* function for *DHCP Snooping*.

Possible values:

- `marked`
  The *Auto-Disable* function for *DHCP Snooping* is active.
  Also mark the checkbox in the *Auto-disable* column on the *Port* tab in the *Network Security > DHCP Snooping > Configuration* dialog for the relevant ports.
- `unmarked` (default setting)
  The *Auto-Disable* function for *DHCP Snooping* is inactive.

Binding database

Remote file name

Specifies the name of the file in which the device saves the DHCP Snooping binding database.

Note:
The device saves only dynamic bindings in the persistent binding database. The device saves static bindings in the configuration profile.

Remote IP address

Specifies the remote IP address under which the device saves the persistent DHCP Snooping binding database. With the value `0.0.0.0` the device saves the binding database locally.

Possible values:

- Valid IPv4 address
- `0.0.0.0` (default setting)
  The device saves the DHCP Snooping binding database locally.

Store interval [s]

Specifies the time delay in seconds after which the device saves the DHCP Snooping binding database when the device identifies a change in the database.

Possible values:

- `15..86400 (1 d)` (default setting: `300`)

4.6.2 DHCP Snooping Configuration

[Network Security > DHCP Snooping > Configuration]

This dialog lets you set up DHCP Snooping for individual ports and for individual VLANs.

The dialog contains the following tabs:
- [Port]
- [VLAN ID]

[Port]

In this tab you set up the *DHCP Snooping* function for individual ports.
- Set up a port as trusted/untrusted.
- Activate/deactivate the logging of invalid packets for individual ports.
- Limit the amount of DHCP packets.
- Deactivate a port automatically if the amount of DHCP data packets exceeds the threshold value.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Trust

Activates/deactivates the security status (trusted, untrusted) of the port.

Possible values:

- `marked`
  The port is set up as trusted. DHCP Snooping forwards permissible client packets through trusted ports.
  Typically, you have connected the trusted port to a DHCP server.
- `unmarked` (default setting)
  The port is set up as untrusted. On untrusted ports, the device compares the receiver port with the client port in the binding database.

Log

Activates/deactivates the logging of invalid packets that the device determines on this port.

Possible values:

- `marked`
  The logging of invalid packets is active.
- `unmarked` (default setting)
  The logging of invalid packets is inactive.

Rate limit

Specifies the maximum number of DHCP packets per burst interval on the port. If the number of incoming DHCP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming DHCP packets.

Possible values:

- `-1` (default setting)
  Deactivates the limitation of the number of DHCP packets per burst interval on this port.
- `0..150` packets per interval
  Limits the maximum number of DHCP packets per burst interval on this port.

You specify the burst interval in the *Burst interval* column.

If you activate the auto-disable function, then the device also disables the port. You find the auto-disable function in the *Auto-disable* column.

Burst interval

Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function.

You specify the maximum number of DHCP packets per burst interval in the *Rate limit* column.

Possible values:

- `1..15` (default setting: `1`)

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *DHCP Snooping* function is monitoring on the port.

Possible values:

- `marked` (default setting)
  The *Auto-Disable* function is active on the port.
  The prerequisite is that in the *Network Security > DHCP Snooping > Global* dialog, in the *Configuration* frame the *Auto-disable* checkbox is marked.
  - If the port receives more DHCP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the 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`
  The *Auto-Disable* function on the port is inactive.

[VLAN ID]

In this tab you set up the *DHCP Snooping* function for individual VLANs.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

VLAN ID

Displays the VLAN ID to which the table row relates.

Active

Activates/deactivates the *DHCP Snooping* function in this VLAN.

The *DHCP Snooping* function forwards valid DHCP client messages to the trusted ports in VLANs without the *Routing* function.

Possible values:

- `marked`
  The *DHCP Snooping* function is active in this VLAN.
- `unmarked` (default setting)
  The *DHCP Snooping* function is inactive in this VLAN.
  The device forwards DHCP packets according to the switching settings without monitoring the packets. The binding database remains unchanged.

Note:
To enable DHCP Snooping for a port, enable the *DHCP Snooping* function globally in the *Network Security > DHCP Snooping > Global* dialog. Verify that you assigned the port to a VLAN in which DHCP Snooping is enabled.

4.6.3 DHCP Snooping Statistics

[Network Security > DHCP Snooping > Statistics]

With DHCP Snooping, the device logs detected errors and generates statistics. In this dialog, you monitor the DHCP Snooping statistics for each port.

The device logs the following:
- Errors detected when validating the MAC address of the DHCP client
- DHCP client messages with a detected incorrect port
- DHCP server messages to untrusted ports

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Reset

Resets the values in the table.

Port

Displays the port number.

MAC verify failures

Displays the number of discrepancies between the MAC address of the DHCP client in the ‘chaddr’ field of the DHCP data packet and the source address in the Ethernet packet.

Invalid client messages

Displays the number of incoming DHCP client messages received on the port for which the device expects the client on another port according to the DHCP Snooping binding database.

Invalid server messages

Displays the number of DHCP server messages the device received on the untrusted port.

4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP Snooping uses DHCP messages to set up and update the binding database.
- Static bindings
  The device lets you enter up to 2048 static DHCP Snooping bindings in the database.
- Dynamic bindings
  The dynamic binding database contains data for clients only on untrusted ports.

This menu lets you specify the settings for static and dynamic bindings.
- Set up new static bindings and set them to active/inactive.
- Display, activate/deactivate or delete static bindings that have been set up.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Opens the *Create* window to add a table row.

In the *MAC address* field, you specify the MAC address which you bind to an IP address and a VLAN ID.

Possible values:

▶ Valid Unicast MAC address
  Specify the value with a colon separator, for example `00:11:22:33:44:55`.

Remove

Removes the selected table row.

The prerequisite is that in the *Active* column the checkbox is unmarked.

Also, the device removes the dynamic bindings of this port set up with the *IP Source Guard* function.

MAC address

Displays the MAC address that you bind to an IP address and a VLAN ID.

IP address

Specifies the IP address for the static DHCP Snooping binding.

Possible values:

- Valid Unicast IPv4 address smaller than `224.x.x.x` and outside the range `127.0.0.0/8` (default setting: `0.0.0.0`)

VLAN ID

Specifies the VLAN ID to which the table row relates.

Possible values:

- `<VLAN IDs of the set-up VLANs>`

Port

Specifies the port for the static DHCP Snooping binding.

Possible values:

- Available ports

Remaining binding time

Displays the remaining time for the dynamic DHCP Snooping binding.

Active

Activates/deactivates the specified static DHCP Snooping binding.

Possible values:

- `marked`
  The static DHCP Snooping binding is active.
  The prerequisite is that in the *Time > Basic Settings* dialog the date and time are set correctly in the device. Otherwise, the bindings may get lost after rebooting the device.
- `unmarked` (default setting)
  The static DHCP Snooping binding is inactive.

4.7 IP Source Guard

[Network Security > IP Source Guard]

The *IP Source Guard* function (IPSG) supports the network security. The function filters IP data packets based on the source ID (source IP address or source MAC address) of the subscriber. IPSG supports you in protecting the network against attacks through IP/MAC address spoofing.

IPSG and DHCP Snooping
The *IP Source Guard* function operates in combination with the port *DHCP Snooping* function.

The *DHCP Snooping* function discards IP data packets on untrusted ports, except DHCP messages. When the device receives DHCP responses and the DHCP Snooping binding database is set up, the device generates a VLAN Access Control List (VACL) for each port containing the source IDs of the subscribers.

You specify the parameters of the *DHCP Snooping* function for individual ports and VLANs in the *Network Security > DHCP Snooping > Configuration* dialog.

IPSG and port security
The *IP Source Guard* function cooperates with the *Port Security* function. See the *Network Security* > Port Security dialog. Upon request, IPSG informs the *Port Security* function on request if a MAC address belongs to a valid binding.

- If you deactivated IPSG on the ingress port, then IPSG identifies the data packet as valid.
- If you activated IPSG on the ingress port, then IPSG checks the MAC address using the bindings database. If the MAC address is entered in the bindings database, then IPSG identifies the data packet as valid, or otherwise invalid.

The *Port Security* function takes over the subsequent processing of invalid data packets. You specify the settings of the *Port Security* function in the *Network Security > Port Security* dialog.

Note:
For the device to check the IP address and the MAC address of the source of the data packets received on the port, enable the *Verify MAC* function.
For the device to check the VLAN ID and the MAC address of the source before forwarding the data packet, additionally enable the *Port Security* function. See the *Network Security > Port Security* dialog.

The menu contains the following dialogs:

- IP Source Guard Port
- IP Source Guard Bindings

4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

This dialog lets you display and set up the following device properties for each port:
- Include/exclude source MAC addresses for the filtering.
- Activate/deactivate the *IP Source Guard* function.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Verify MAC

Activates/deactivates the filtering based on the source MAC address if the *IP Source Guard* function is active. The device executes this filtering in addition to the filtering based on the source IP address.

Possible values:

- `marked`
  Filtering based on the source MAC address is active.
  To activate the function, mark the *Active* checkbox.
- `unmarked` (default setting)
  Filtering based on the source MAC address is inactive.
  To deactivate the function, also unmark the *Active* checkbox.

Active

Activates/deactivates the *IP Source Guard* function on the port.

Possible values:

- `marked`
  The *IP Source Guard* function is active.
  You also enable the *DHCP Snooping* function in the *Network Security > DHCP Snooping > Global* dialog.
- `unmarked` (default setting)
  The *IP Source Guard* function is inactive.

4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

This dialog displays static and dynamic *IP Source Guard Bindings* settings.

- The device learns dynamic bindings through DHCP Snooping. See the *Network Security > DHCP Snooping > Configuration* dialog.
- Static bindings are *IP Source Guard Bindings* settings manually set up by the user. The dialog lets you edit static bindings.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *MAC address* field, you specify the MAC address for the static binding.
- In the *IP address* field, you specify the IP address for the static binding.
- In the *VLAN ID* field, you specify the VLAN ID.
- From the *Port* drop-down list, you select the port number.


Remove

Removes the selected table row.

The prerequisite is that in the *Active* column the checkbox is unmarked.

MAC address

Displays the MAC address of the binding.

IP address

Displays the IP address of the binding.

VLAN ID

Displays the VLAN ID of the binding.

Port

Displays the number of the port of the binding.

Hardware status

Displays the hardware status of the binding.

The device applies the binding to the hardware only if the settings are correct. Before the device applies the static IPSG binding to the hardware, it checks the following prerequisites:

- The *Active* checkbox is marked.
- The *IP Source Guard* function on the port is active, in the *Network Security > IP Source Guard > Port* dialog the *Active* checkbox is marked.

Possible values:

- `marked`
  The binding is active, the device applies the binding to the hardware.
- `unmarked`
  The binding is inactive.

Active

Activates/deactivates the specified static IPSG binding between the specified MAC address and the specified IP address, for the specified VLAN on the specified port.

Possible values:

- `marked`
  The static IPSG binding is active.
- `unmarked` (default setting)
  The static IPSG binding is inactive.

Note:
To make the static binding effective, activate the *IP Source Guard* function on the corresponding port. In the *Network Security > IP Source Guard > Port* dialog, mark the *Active* checkbox.

4.8 Dynamic ARP Inspection

[Network Security > Dynamic ARP Inspection]

Dynamic ARP Inspection is a function that supports the network security. This function analyzes ARP packets, logs them, and discards invalid and hostile ARP packets.

The *Dynamic ARP Inspection* function helps prevent a range of man-in-the-middle attacks. With this kind of attack, a hostile station listens in on the data stream from other subscribers by encroaching on the ARP cache of its unsuspecting neighbors. The hostile station sends ARP requests and ARP responses and enters the IP address of another subscriber for its own MAC address in the IP-to-MAC address relationship (binding).

Using the following measures, the *Dynamic ARP Inspection* function helps ensure that the device only forwards valid ARP requests and ARP responses.

- Listening in on ARP requests and ARP responses on untrusted ports.
- Verifying that the determined packets have a valid IP to MAC address relationship (binding) before the device updates the local ARP cache and before the device forwards the packets to the related destination address.
- Discarding invalid ARP packets.

The device lets you specify up to 100 active ARP ACLs (access lists). You can activate up to 20 rules for each ARP ACL.

The menu contains the following dialogs:

- Dynamic ARP Inspection Global
- Dynamic ARP Inspection Configuration
- Dynamic ARP Inspection ARP Rules
- Dynamic ARP Inspection Statistics

4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

Configuration

Verify source MAC

Activates/deactivates the source MAC address verification. The device executes the check in both ARP requests and ARP responses.

Possible values:

- `marked`
  The source MAC address verification is active.
  The device checks the source MAC address of the received ARP packets.
  - The device transmits ARP packets with a valid source MAC address to the related destination address and updates the local ARP cache.
  - The device discards ARP packets with an invalid source MAC address.
- `unmarked` (default setting)
  The source MAC address verification is inactive.

Verify destination MAC

Activates/deactivates the destination MAC address verification. The device executes the check in ARP responses.

Possible values:

- `marked`
  The destination MAC address verification is active.
  The device checks the destination MAC address of the incoming ARP packets.
  - The device transmits ARP packets with a valid destination MAC address to the related destination address and updates the local ARP cache.
  - The device discards ARP packets with an invalid destination MAC address.
- `unmarked` (default setting)
  The checking of the destination MAC address of the incoming ARP packets is inactive.

Verify IP address

Activates/deactivates the IP address verification.

In ARP requests, the device checks the source IP address. In ARP responses, the device checks the destination and source IP address.

The device designates the following IP addresses as invalid:

- `0.0.0.0`
- Broadcast addresses `255.255.255.255`
- Multicast addresses `224.0.0.0/4` (Class D)
- Class E addresses `240.0.0.0/4` (reserved for subsequent purposes)
- Loopback addresses in the range `127.0.0.0/8`.

Possible values:

- `marked`
  The IP address verification is active.
  The device checks the IP address of the incoming ARP packets. The device transmits ARP packets with a valid IP address to the related destination address and updates the local ARP cache. The device discards ARP packets with an invalid IP address.
- `unmarked` (default setting)
  The IP address verification is inactive.

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Dynamic ARP Inspection*.

Possible values:

- `marked`
  The *Auto-Disable* function for *Dynamic ARP Inspection* is active.
  Also mark the checkbox in the *Port* column on the *Auto-disable* tab in the *Network Security* > Dynamic ARP Inspection > *Configuration* dialog for the relevant ports.
- `unmarked` (default setting)
  The *Auto-Disable* function for *Dynamic ARP Inspection* is inactive.

4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

The dialog contains the following tabs:
- [Port]
- [VLAN ID]

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Trust

Activates/deactivates the monitoring of ARP packets on untrusted ports.

Possible values:

- `marked`
  Monitoring is active.
  The device monitors ARP packets on untrusted ports.
  The device immediately forwards ARP packets on trusted ports.
- `unmarked` (default setting)
  Monitoring is inactive.

Rate limit

Specifies the maximum number of ARP packets per interval on this port. If the rate of incoming ARP packets is currently exceeding the specified limit in a burst interval, then the device discards the additional incoming ARP packets. You specify the burst interval in the *Burst interval* column.

Optionally, the device also deactivates the port if you activate the auto-disable function. You enable/disable the *Auto-Disable* function in the *Auto-disable* column.

Possible values:

- `-1` (default setting)
  Deactivates the limitation of the number of ARP packets per burst interval on this port.
- `0..300` packets per interval
  Limits the maximum number of ARP packets per burst interval on this port.

Burst interval

Specifies the length of the burst interval in seconds on this port. The burst interval is relevant for the rate limiting function.

You specify the maximum number of ARP packets per burst interval in the *Rate limit* column.

Possible values:

- `1..15` (default setting: `1`)

Auto-disable

Activates/deactivates the *Auto-Disable* function for the parameters that the *Dynamic ARP Inspection* function is monitoring on the port.

Possible values:

- `marked` (default setting)
  The *Auto-Disable* function is active on the port.
  The prerequisite is that in the *Network Security > Dynamic ARP Inspection > Global* dialog, in the *Configuration* frame the *Auto-disable* checkbox is marked.
  - If the port receives more ARP packets than specified in the *Rate limit* field in the time specified in the *Burst interval* column, then the device disables the 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`
  The *Auto-Disable* function on the port is inactive.

[VLAN ID]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

VLAN ID

Displays the VLAN ID to which the table row relates.

Log

Activates/deactivates the logging of invalid ARP packets that the device determines in this VLAN. If the device detects an error when checking the IP, source MAC or destination MAC address, or when checking the IP-to-MAC address relationship (binding), then the device identifies an ARP packet as invalid.

Possible values:

- `marked`
  The logging of invalid packets is active.
  The device registers invalid ARP packets.
- `unmarked` (default setting)
  The logging of invalid packets is inactive.

Binding check

Activates/deactivates the checking of incoming ARP packets that the device receives on untrusted ports and on VLANs for which the *Dynamic ARP Inspection* function is active. For these ARP packets the device checks the ARP ACL and the DHCP Snooping relationship (bindings).

Possible values:

- `marked` (default setting)
  The binding check of ARP packets is active.
- `unmarked`
  The binding check of ARP packets is inactive.

Strict ACL check

Activates/deactivates the strict checking of incoming ARP packets based on the ARP ACL rules specified.

Possible values:

- `marked`
  The strict checking is active.
  The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ACL* column.
- `unmarked` (default setting)
  The strict checking is inactive.
  The device checks the incoming ARP packets based on the ARP ACL rule specified in the *ACL* column and subsequently on the entries in the DHCP Snooping database.

ACL

Specifies the ARP ACL that the device uses.

Possible values:

- `<rule name>`
  You add and edit the rules in the *Network Security > Dynamic ARP Inspection > ARP Rules* dialog.

Active

Activates/deactivates the *Dynamic ARP Inspection* function in this VLAN.

Possible values:

- `marked`
  The *Dynamic ARP Inspection* function is active in this VLAN.
- `unmarked` (default setting)
  The *Dynamic ARP Inspection* function is inactive in this VLAN.

4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

This dialog lets you specify rules for checking and filtering ARP packets.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Add

Opens the *Create* window to add a table row.

- From the *Name* drop-down list, you select the name of the ARP rule or specify a new name. Enter the name in the search box.
  - To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  - To add a name: Enter the name in the search box, then click the *Create* link below the search box.
- In the *Source IP address* field, you specify the source IP address of the ARP rule.
- In the *Source MAC address* field, you specify the source MAC address of the ARP rule.

 Remove

Removes the selected table row.

Name

Displays the name of the ARP rule.

Source IP address

Specifies the source address of the IP data packets to which the device applies the rule.

Possible values:

- Valid IPv4 address
  The device applies the rule to IP data packets with the specified source address.

Source MAC address

Specifies the source address of the MAC data packets to which the device applies the rule.

Possible values:

- Valid MAC address
  The device applies the rule to MAC data packets with the specified source address.

Active

Activates/deactivates the *ARP* rule.

Possible values:

- `marked` (default setting)
  The rule is active.
- `unmarked`
  The rule is inactive.

4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

This window displays the number of discarded and forwarded ARP packets in an overview.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Reset

Resets the values in the table.

VLAN ID

Displays the VLAN ID to which the table row relates.

Packets forwarded

Displays the number of ARP packets that the device forwards after checking them using the *Dynamic ARP Inspection* function.

Packets dropped

Displays the number of ARP packets that the device discards after checking them using the *Dynamic ARP Inspection* function.

DHCP drops

Displays the number of ARP packets that the device discards after checking the DHCP Snooping relationship (binding).

DHCP permits

Displays the number of ARP packets that the device forwards after checking the DHCP Snooping relationship (binding).

ACL drops

Displays the number of ARP packets that the device discards after checking them using the ARP ACL rules.

ACL permits

Displays the number of ARP packets that the device forwards after checking them using the ARP ACL rules.

Bad source MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the source MAC address.

Bad destination MAC

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the destination MAC address.

Invalid IP address

Displays the number of ARP packets that the device discards after the *Dynamic ARP Inspection* function detected an error in the IP address.

4.9 ACL

[Network Security > 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 applicable rule to the data stream. The device ignores the rules that follow the first applicable rule. Possible actions include:

- `permit`: The device forwards the data packet to a port or to a VLAN.
  When necessary, the device forwards a copy of the data packets to a further port.
- `deny`: The device drops the data packet.

In the default setting, the device forwards every data packet. As soon as 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 time profile if necessary. See the *Time > Time Profile* dialog. The device applies Access Control Lists with a time profile at specified times instead of permanently.
- ☐ 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

4.9.1 ACL IPv4 Rule

[Network Security > 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 numerically 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
- Classification according to DSCP
- Classification according to ToS

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Opens the *Create* window to add a table row.

- From the *Group name* drop-down list, you select the Access Control List name to which the rule belongs or add a new name.
  To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  To add a name: Enter the name in the search box, then click the *Create* link below the search box. The following rules apply:
  – You can enter an ASCII character string with 1..31 characters.
  – The first character needs to be a letter.
  – The device accepts the following characters:
  ```
  a..z
  A..Z
  0..9
  -._
  ```
- 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.

You specify the name when adding a table row.

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 numerically 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*
  - *ICMP type*, *ICMP code*
  - *IGMP type*
  - *Established*
  - *Packet fragmented*
  - *TCP flag*

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 that contain the specified value in the *Protocol* field.

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 (2¹⁶-1)`
  The device applies the rule only to IP data packets containing the specified source port.
  To specify a port range, you can use one of the following operators:
  - `<`
    Range below the specified port number
  - `>`
    Range above the specified port number
  - `!=`
    Entire port range except the specified port

  These operators are allowed only in rules which the device applies to the received data packets.
  See the *Network Security > ACL > Assignment* dialog: *Direction* column = *inbound*.

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 (2¹⁶-1)`
  The device applies the rule only to IP data packets containing the specified destination port.
  To specify a port range, you can use one of the following operators:
  - `<`
    Range below the specified port number
  - `>`
    Range above the specified port number
  - `!=`
    Entire port range except the specified port

  These operators are allowed only in rules which the device applies to the received data packets. See the *Network Security > ACL > Assignment* dialog: *Direction* column = *inbound*.

DSCP

Specifies the Differentiated Service Code Point (DSCP value) in the header of the IP data packets to which the device applies the rule.

Possible values:

- `-` (default setting)
  The device applies the rule to every IP data packet without evaluating the DSCP value.
- `0..63`
  The device applies the rule only to IP data packets containing the specified DSCP value.

TOS priority

Specifies the *IP Precedence (ToS)* value in the header of the IP data packets to which the device applies the rule.

Possible values:

- `any` (default setting)
  The device applies the rule to every IP data packet without evaluating the *ToS* value.
- `0..7`
  The device applies the rule only to IP data packets containing the specified *ToS* value.

TOS mask

Specifies the bit mask for the *ToS* value in the header of the IP data packets to which the device applies the rule. The prerequisite is that in the *TOS priority* column a *ToS* value is specified.

Possible values:

- `any` (default setting)
  The device applies the rule to IP data packets and evaluates the *ToS* value completely.
- `1..1f`
  The device applies the rule to IP data packets and evaluates the bits of the *ToS* value specified in the bit mask.

ICMP type

Specifies the ICMP type in the TCP header of the IP data packets to which the device applies the rule.

Possible values:

- `-1` (default setting)
  ICMP type matching is inactive.
- `0..255`
  The device applies the rule to every IP data packet and evaluates the specified ICMP type.

ICMP code

Specifies the ICMP code in the TCP header of the IP data packets to which the device applies the rule. The prerequisite is that in the *ICMP type* field an ICMP value is specified.

Possible values:

- `-1` (default setting)
  ICMP code matching is inactive.
- `0..255`
  The device applies the rule to every IP data packet and evaluates the specified ICMP code.

IGMP type

Specifies the IGMP type in the TCP header of the IP data packets to which the device applies the rule.

Possible values:

- `0` (default setting)
  IGMP type matching is inactive.
- `1..255`
  The device applies the rule to every IP data packet and evaluates the specified IGMP type.

Established

Activates/deactivates applying the ACL rule to TCP data packets which have either the RST bit, or the ACK bit set in the TCP header.

Possible values:

- `marked`
  The device applies the rule to every IP data packet in which the RST bit, or the ACK bit is set in the TCP header.
- `unmarked` (default setting)
  Matching is inactive.

Packet fragmented

Activates/deactivates applying the ACL rule to the packet fragments.

To filter the complete data packet including its fragments, add 2 ACL rules.

- Create an ACL rule for the initial data packet to filter on both at the protocol level and at the TCP/UDP ports.
- Create a second ACL rule for the fragments to filter only at the protocol level.

Possible values:

- `marked`
  The device applies the ACL rule to the fragments. Use this setting in the second ACL rule for the fragments.
- `unmarked` (default setting)
  The device does not apply the ACL rule to the fragments.

TCP flag

Specifies the TCP flag and mask value.

The device lets you enter multiple values, by separating the values with a comma.

Specify the flags as either `+` or `-`.

Possible values:

- `-` (default setting)
  TCP flag matching is inactive.
- `-`
  When you use this value in combination with the following flags, the device evaluates packets in which the flag is not set.
- `+`
  When you use this value in combination with the following flags, the device evaluates packets in which the flag is set.
- `fin`
  Indicates that the sending device has finished its transmission.
- `syn`
  Indicates that the `Synchronize sequence` numbers are significant. Only the first packet sent from each end device has this flag set.
- `rst`
  Indicates a reset of the TCP connection.
- `psh`
  Indicates the push function, in which a device asks to push the buffered data to the receiving application.
- `ack`
  Indicates that the `Acknowledgment` field is significant. Every packet, after the initial syn packet sent by the client, has this flag set.
- `urg`
  Indicates that the `Urgent pointer` field is significant.

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.

Redirection port

Specifies the port to which the device forwards the IP data packets. The prerequisite is that in the *Action* column the value `permit` is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries.

Possible values:

- `-` (default setting)
  The *Redirection port* function is inactive.
- `<Port number>`
  The device forwards the IP data packets to the specified port.

Mirror port

Specifies the port to which the device forwards a copy of the IP data packets. The prerequisite is that in the *Action* column the value `permit` is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries.

Possible values:

- `-` (default setting)
  The *Mirror port* function is inactive.
- `<Port number>`
  The device forwards a copy of the IP data packets to the specified port.

Assigned queue ID

Specifies the priority queue to which the device assigns the IP data packets.

Possible values:

- `-` (default setting)
- `0..7`

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.

Time profile

Specifies if the device applies the rule permanently or time-controlled.

Possible values:

- `<empty>` (default setting)
  The device applies the rule permanently.
- `[Time Profile]`
  The device applies the rule only at the times specified in the selected time profile. You edit the time profiles in the *Time > Time Profile* dialog.
  The implied *Deny-All* rule of the ACLs is permanently valid independently of the time control.

Rate limit

Specifies the limit for the data transfer rate for the port specified in the *Redirection port* column. The limit applies to the summary of the data sent and received.

This function limits the data stream on the port or in the VLAN:

Possible values:

- `0` (default setting)
  No limitation of the data transfer rate.
- `1..4294967295 (2³²-1)`
  If the data transfer rate on the port exceeds the value specified, then the device discards superfluous IP data packets. The prerequisite is that in the *Burst size* column a value >`0` is specified. You specify the measurement unit of the limit in the *Unit* column.

Unit

Specifies the measurement unit for the data transfer rate specified in the *Rate limit* column.

Possible values:

- *kbps*
  kBytes per second

Burst size

Specifies the limit in KByte for the data volume during temporary bursts.

Possible values:

- `0` (default setting)
  No limitation of the data volume.
- `1..128`
  If during temporary bursts on the port the data volume exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the *Rate limit* column a value >`0` is specified.

Recommendation:

- If the bandwidth is known:
  Burst size = bandwidth × allowed duration of a burst / 8
- If the bandwidth is unknown:
  Burst size = 10 × MTU (*Maximum Transmission Unit*) of the port

4.9.2 ACL MAC Rule

[Network Security > 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 numerically 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
- Type of the transmitting protocol
- Membership of a specific VLAN
- Service class of a data packet

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Opens the *Create* window to add a table row.

- From the *Group name* drop-down list, you select the Access Control List name to which the rule belongs or add a new name.
  To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  To add a name: Enter the name in the search box, then click the *Create* link below the search box. The following rules apply:
  - You can enter an ASCII character string with 1..31 characters.
  - The first character needs to be a letter.
  - The device accepts the following characters:
    ```
    a..z
    A..Z
    0..9
    -._
    ```
- 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.

You specify the name when adding a table row.

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 numerically 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*
  - *Ethertype*
  - *Ethertype custom value*
  - *VLAN ID*
  - *COS*

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 `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a source address in the range from `00:11:22:33:44:54` to `…: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 source address. The bit mask lets you specify the address range with bit-level accuracy.
  Example `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: The device applies the rule to MAC data packets with a destination address in the range from `00:11:22:33:44:54` to `…:57`.

Ethertype

Specifies the *Ethertype* keyword of the MAC data packets to which the device applies the rule.

Possible values:

- *custom* (default setting)
  The device applies the value specified in the *Ethertype custom value* column.
- *appletalk*
- *arp*
- *ibmsna*
- *ipv4*
- *ipv6*
- *ipxold*
- *mplsmcast*
- *mplsucast*
- *netbios*
- *novell*
- *rarp*
- *pppoe*

Ethertype custom value

Specifies the *Ethertype* value of the MAC data packets to which the device applies the rule. The prerequisite is that in the *Ethertype* column the value *custom* is specified.

Possible values:

- `0` (default setting)
  The device applies the rule to every MAC data packet without evaluating the *Ethertype* value.
- `600..ffff`
  The device applies the rule only to MAC data packets that contain the *Ethertype* value specified here.

VLAN ID

Specifies the VLAN ID of the MAC data packets to which the device applies the rule.

Possible values:

- `0` (default setting)
  The device applies the rule to every MAC data packet without evaluating the VLAN ID.
- `1..4042`

COS

Specifies the Class of Service (COS) value of the MAC data packets to which the device applies the rule.

Possible values:

- `0..7`
- `any` (default setting)
  The device applies the rule to every MAC data packet without evaluating the Class of Service value.

Note:
For data packets without a VLAN tag, the device uses the *Port priority* instead of the *COS* value.

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.

Redirection port

Specifies the port to which the device forwards the MAC data packets. The prerequisite is that in the *Action* column the value *permit* is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries.

Possible values:

- `-` (default setting)
  The *Redirection port* function is inactive.
- `<Port number>`
  The device forwards the MAC data packets to the specified port.

Mirror port

Specifies the port to which the device forwards a copy of the MAC data packets. The prerequisite is that in the *Action* column the value *permit* is specified. The device does not provide the option of mirroring IP data packets across VLAN boundaries.

Possible values:

- `-` (default setting)
  The *Mirror port* function is disabled.
- `<Port number>`
  The device forwards a copy of the MAC data packets to the specified port.

Assigned queue ID

Specifies the ID of the priority queue to which the device forwards the MAC data packets.

Possible values:

- `-` (default setting)
- `0..7`

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.

Time profile

Specifies if the device applies the rule permanently or time-controlled.

Possible values:

- `<empty>` (default setting)
  The device applies the rule permanently.
- `[Time Profile]`
  The device applies the rule only at the times specified in the selected time profile. You edit the time profiles in the *Time > Time Profile* dialog.
  The implied *Deny-All* rule of the ACLs is permanently valid independently of the time control.

Rate limit

Specifies the limit for the data transfer rate for the port specified in the *Redirection port* column. The limit applies to the summary of the data sent and received.

This function limits the data stream on the port or in the VLAN:

Possible values:

- `0` (default setting)
  No limitation of the data transfer rate.
- `1..4294967295 (2³²-1)`
  If the data transfer rate on the port exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the *Burst size* column a value >`0` is specified. You specify the measurement unit of the limit in the *Unit* column.

Unit

Specifies the measurement unit for the data transfer rate specified in the *Rate limit* column.

Possible values:

- *kbps*
  kBytes per second

Burst size

Specifies the limit in KByte for the data volume during temporary bursts.

Possible values:

- `0` (default setting)
  No limitation of the data volume.
- `1..128`
  If during temporary bursts on the port the data volume exceeds the value specified, then the device discards superfluous MAC data packets. The prerequisite is that in the *Rate limit* column a value >`0` is specified.

Recommendation:

- If the bandwidth is known:
  Burst size = bandwidth × allowed duration of a burst / 8
- If the bandwidth is unknown:
  Burst size = 10 × MTU (*Maximum Transmission Unit*) of the port

4.9.3 ACL Assignment

[Network Security > 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 device lets you specify a maximum of 100 ACLs, which can each contain a certain number of rules. The number of rules that you can actually assign to the ports and VLANs might be smaller than the number of rules specified in the device. An example in the “Configuration” user manual illustrates the factors that affect the possible number that you can actually assign.

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*) or sent (*outbound*).

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. Access to the device management is only possible using the Command Line Interface through the serial connection.

Note:
You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Add

Opens the *Create* window to assign a rule to a port or a VLAN.
- From the *Port/VLAN* drop-down list, you select the port or the VLAN 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.

- From the *Direction* drop-down list, you select if the device applies the rule to received or sent data packets.
- From the *Group name* drop-down list, you select the rule that 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.

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.

You edit Access Control Lists with IPv4 rules in the *Network Security > ACL > IPv4 Rule* dialog. You edit Access Control Lists with MAC rules in the *Network Security > ACL > MAC Rule* dialog.

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 if the device applies the Access Control List to received or sent data packets.

Possible values:

- *inbound*
  The device applies the Access Control List to data packets received on the port or in the VLAN.
- *outbound*
  The device applies the Access Control List to data packets sent on the port or in the VLAN.

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 (2³²-1)`

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

[Switching > Global]

This dialog lets you specify the following settings:

- Change the Aging time of the MAC address table (forwarding database) entries
- 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 superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to a buffer overflow on a port. Shortly before the buffer memory of a port 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.

The connected devices then stop sending data packets for the duration of the signaling. On an uplink port, this can possibly cause undesired sending interruptions in the higher-level network segment (“wandering backpressure”). The flow control mechanism thus lowers the network to the bandwidth that the slowest device in the network can process.

According to IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN ≥1. However, a few 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 MAC address table (forwarding database).

You find the MAC address table (forwarding database) 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 the network require this, then activate the function.

Possible values:

- `marked`
  The device operates in the *VLAN-unaware* mode according to IEEE 802.1Q:
  - The device ignores the VLAN settings in the device and the VLAN ID in the data packets. The device forwards 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 `1` 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 according to IEEE 802.1Q:
  - The device evaluates the VLAN tags in the data packets.
  - The device forwards 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 a 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

[Switching > 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 18.

Port

Displays the port number.

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.

Broadcast threshold

Specifies the threshold value for received broadcasts on this port.

Possible values:

- `0..14880000` (default setting: `0`)
  The value `0` deactivates the rate limiter function on this port.
  - If you select the value *`percent`* in the *Unit* column, then enter a percentage value from `1` to `100`.
  - If you select the value *`pps`* in the *Unit* column, then enter an absolute value for the data rate.

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.

Multicast threshold

Specifies the threshold value for received multicasts on this port.

Possible values:

- `0..14880000` (default setting: `0`)
  The value `0` deactivates the rate limiter function on this port.
  - If you select the value *`percent`* in the *Unit* column, then enter a percentage value from `0` to `100`.
  - If you select the value *`pps`* in the *Unit* column, then enter an absolute value for the data rate.

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.

Unicast threshold

Specifies the threshold value for received unicasts with an unknown destination address on this port.

Possible values:

- `0..14880000` (default setting: `0`)
  The value `0` deactivates the rate limiter function on this port.
  - If you select the value *`percent`* in the *Unit* column, then enter a percentage value from `0` to `100`.
  - If you select the value *`pps`* in the *Unit* column, then enter an absolute value for the data rate.

[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 18.

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

[Switching > Filter for MAC Addresses]

This dialog lets you display and edit address filters for the MAC address table (forwarding database). 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 forwards the data packets as follows:
- When the table contains the destination address of a data packet, the device forwards the data packet from the receiving port to the port specified in the table row.
- When there is no table row for the destination address, the device forwards the data packet from the receiving port to every other port.

Table

To delete the learned MAC addresses from the MAC address table (forwarding database), click in the *Basic Settings > Restart* dialog the *Clear FDB* button.

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Opens the *Create* window to add a table row.
- In the *MAC address* field, you specify the destination MAC address.
- In the *VLAN ID* field, you specify the VLAN ID.
- In the list field, you select the ports.
  - If the destination MAC address is a unicast address, select exactly one port.
  - If the destination MAC address is a multicast or broadcast address, select one or more ports.
  - Do not select a port to add a *Discard* filter. The device discards data packets with the destination MAC address specified in the table row.

Remove

Removes the selected table row.

Clear FDB

Deletes the MAC addresses from the forwarding table that have the value *Learned* in the *Status* column.

MAC address

Displays the destination MAC address to which the table row relates.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

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:

- `Static`
  Address filter set up manually
  The address filter stays set up permanently.
  You can edit or delete an address filter with the status `Static`.
- *Mgmt*
  MAC address of the device
  The address filter is protected against changes.
- *Learned*
  Address filter set up automatically
  The device set up the filter based on received data packets.
  The device deletes an address filter with the status *Learned* after a particular time (*Aging time [s]*) when the device no longer receives data packets from the respective MAC address.
  To edit or delete an address filter with the status *Learned*, first set its status to `Static` and save this change to the volatile memory.
- *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.
- *Other*
  Static address filter
  One of the following device functions has set up the destination address:
  - *802.1X*
  - *Port Security*

<Port number>

Displays how the corresponding port sends data packets to the destination address given in the leftmost column. The table cell contains an abbreviation. When you hover the mouse pointer over or tap a table cell, a tooltip displays the full text.

Possible values:

- `-`
  Tooltip: `-`
  The port does not send any data packets to the destination address.
- `L`
  Tooltip: `Learned`
  The port sends data packets to the destination address.
  The device has automatically set up the filter based on received data packets.
- *US*
  Tooltip: *Unicast static*
  The port sends data packets to the unicast destination address.
  A user has set up the filter.

- *MS*
  Tooltip: *Multicast static*
  The port sends data packets to the multicast destination address.
  A user has set up the filter.
- *FA*
  Tooltip: *Forward all*
  The port sends all multicast data packets.
  The device has automatically set up the filter based on received data packets.
- *IL*
  Tooltip: *IGMP learned*
  The port sends data packets to the multicast destination address.
  The *IGMP Snooping* function in the device has set up the filter.
- *MS/IL*
  Tooltip: *Multicast static/IGMP learned*
  The port sends data packets to the multicast destination address.
  A user has set up the filter. Additionally, the *IGMP Snooping* function in the device has set up the filter.
- *GL*
  Tooltip: *GMRP learned*
  The port sends data packets to the multicast destination address.
  The *GMRP* function in the device has set up the filter.
- *GFA*
  Tooltip: *GMRP forward all*
  The port sends group-addressed multicast data packets.
  A user has set up the filter, or the *GMRP* function in the device has set up the filter.
- *MS/GL*
  Tooltip: *Multicast static/GMRP learned*
  The port sends data packets to the multicast destination address.
  A user has set up the filter. Additionally, the *GMRP* function in the device has set up the filter.
- *ML*
  Tooltip: *MMRP learned*
  The port sends data packets to the multicast destination address.
  The *MMRP* function in the device has set up the filter.
- *MS/ML*
  Tooltip: *Multicast static/MMRP learned*
  The port sends data packets to the multicast destination address.
  A user has set up the filter. Additionally, the *MMRP* function in the device has set up the filter.

5.4 IGMP Snooping

[Switching > 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 forwards the Multicast data packets to every port.
- With the activated IGMP Snooping function, the device forwards 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 generates 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 MAC address table (forwarding database). When a multicast receiver joins a multicast group, the device adds 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

[Switching > IGMP Snooping > Global]

This dialog lets you enable the *IGMP Snooping* function in the device and set the function up for each port and each VLAN.

Operation

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

Deletes the IGMP Snooping entries and resets the counter in the *Information* frame to `0`.

Processed multicast controls

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 set up the MAC address table (forwarding database) for transmitting the Multicast data packets.

Possible values:

- `0..2147483647 (2³¹-1)`

You use the *Clear 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

[Switching > IGMP Snooping > Configuration]

This dialog lets you enable the *IGMP Snooping* function in the device and set the function up for each port and each VLAN.

The dialog contains the following tabs:
- [VLAN ID]
- [Port]

[VLAN ID]

In this tab you set up 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 18.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

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 MAC address table (forwarding database) 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 MAC address table (forwarding database).
- `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 set up the *IGMP Snooping* function for every port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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` (default setting)
  IGMP Snooping is active on this port. The device includes the port in the multicast data stream.
- `unmarked`
  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 MAC address table (forwarding database) 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 MAC address table (forwarding database).
- `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 set-up VLANs.
  If you use the *RCP* function and the device operates as slave, then do not activate the *Static query port* mode for the ports on the secondary ring/network.
- `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 relates.

5.4.3 IGMP Snooping Enhancements

[Switching > IGMP Snooping > Snooping Enhancements]

This dialog lets you select a port for a VLAN and to set up the port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Wizard

Opens the *Wizard* window that helps you select and set up the ports. See “[Wizard: IGMP snooping enhancements]” on page 261.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

<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.
- `L` = 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 set up query port.
- `S` = 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 set-up query ports.
  To assign this value, perform the following steps:
  - ☐ Open the *Wizard* window.
  - ☐ On the *Configuration* page, mark the *Static* checkbox.
- `A` = Automatic
  The device detected the port as a query port. The prerequisite is that you set up the port as *Learn by LLDP*.

- 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 forwards every received Multicast stream in the VLAN to this port. Use this setting for diagnostic 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

Enhances the clarity of the display. The table emphasizes the cells which contain the specified value. This helps to analyze and sort the table according to your needs.

Possible values:

- *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 set up 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 VLAN ID.

Port

Select the ports.

Configuration

VLAN ID

Displays the selected VLAN ID.

Port

Displays the number of the selected ports.

Static

Specifies the port as a static query port in the set-up VLANs. 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 sends on this port every data packet with a Multicast address in the destination address field.

5.4.4 IGMP Snooping Querier

[Switching > IGMP Snooping > Querier]

The device forwards a Multicast stream only to those ports to which a Multicast receiver is connected.

To detect which ports Multicast receivers are connected to, the device sends query data packets on the ports at a given 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 set up the Snooping Querier settings globally and for the set-up VLANs.

Operation

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 itself generates *General Query* data packets when it has received query data packets from the Multicast router.

Possible values:

- `1..1800` (default setting: `60`)

Expiry 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 set-up VLANs.

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

Active

Activates/deactivates the IGMP Snooping Querier function for this VLAN.

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.

Current state

Displays if the Snooping Querier is active for this VLAN.

Possible values:

- `marked`
  The Snooping Querier is active for this VLAN.
- `unmarked`
  The Snooping Querier is inactive for this VLAN.

IP 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 Internet Group Management Protocol (IGMP) 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

[Switching > IGMP Snooping > Multicasts]

The device lets you specify how it forwards data packets with unknown Multicast addresses: Either the device discards these data packets, floods them to every port, or forwards them only to the ports that previously received query packets.

The device also forwards 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 Multicast address.
- *Send to all ports* (default setting)
  The device forwards data packets with an unknown MAC Multicast address to every port.
- *Send to query ports*
  The device forwards data packets with an unknown MAC Multicast address to the query ports.

Table

In the table you specify the settings for known Multicasts for the set-up VLANs.

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

VLAN ID

Displays the ID of the VLAN to which the table row relates.

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

[Switching > MRP-IEEE]

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP-IEEE) to replace the Generic Attribute Registration Protocol (GARP). The IEEE standards association 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

[Switching > MRP-IEEE > Configuration]

This dialog lets you set the various MRP-IEEE timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdrawals 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 *Leave* timer value `≥ (2x JoinTime) + 60`.
- To minimize the volume of *Rejoin* data packets the device generates following a *LeaveAll* event, specify the value for the *LeaveAll* timer larger than the *Leave* timer value.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Join time [1/100s]

Specifies the *Join* timer which controls the interval between transmit opportunities applied to the Applicant state machine.

Possible values:

▶ `10..100` (default setting: `20`)

Leave time [1/100s]

Specifies the *Leave* timer which controls the period that the Registrar state machine waits in the *Leave (LV)* state before transitioning to the *Empty (MT)* state.

Possible values:

▶ `20..600` (default setting: `60`)

Leave all time [1/100s]

Specifies the *LeaveAll* timer which controls the frequency with which the *LeaveAll* state machine generates *LeaveAll* PDUs.

Possible values:

▶ `200..6000` (default setting: `1000`)

5.5.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

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

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 18.

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 18.

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.

Information

Buttons

Reset statistics

Resets the port statistics counters and the values in the *Last received MAC address* column.

Transmitted MMRP PDU

Displays the number of MMRPDUs transmitted in the device.

Received MMRP PDU

Displays the number of MMRPDUs received in the device.

Received bad header PDU

Displays the number of MMRPDUs received with a bad header in the device.

Received bad format PDU

Displays the number of MMRPDUs with a bad data field that were not transmitted in the device.

Transmission failed

Displays the number of MMRPDUs not transmitted in the device.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Transmitted MMRP PDU

Displays the number of MMRPDUs transmitted on the port.

Received MMRP PDU

Displays the number of MMRPDUs received on the port.

Received bad header PDU

Displays the number of MMRPDUs with a bad header that were received on the port.

Received bad format PDU

Displays the number of MMRPDUs 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 MAC address from which the port last received MMRPDUs.

5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

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 generates 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

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 every 1 s, 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 18.

Port

Displays the port number.

Active

Activates/deactivates the port MVRP participation.

Possible values:

- `marked` (default setting)
  With MVRP enabled globally and on this port, the device distributes VLAN membership information to MVRP-aware devices connected to this port.
- `unmarked`
  Disables the port MVRP participation.

Restricted VLAN registration

Activates/deactivates the *Restricted VLAN registration* function on this port.

Possible values:

- `marked`
  If enabled and a static VLAN registration entry exists, then the device lets you add a dynamic VLAN for this entry.
- `unmarked` (default setting)
  Disables the *Restricted VLAN registration* function on this port.

[Statistics]

Devices on a LAN exchange Multiple VLAN Registration Protocol Data Units (MVRPDUs) 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 18.

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 MAC address from which the port last received MVRPDUs.

5.6 GARP

[Switching > GARP]

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE standards association 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

[Switching > GARP > 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 802.1D.

Operation

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 18.

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

[Switching > GARP > GVRP]

The GARP VLAN Registration Protocol or Generic VLAN Registration Protocol (GVRP) 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 set up devices in a VLAN network.

GVRP is a GARP application that provides IEEE 802.1Q-compliant VLAN pruning, and setting up 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 add and manage VLANs connected through the 802.1Q trunk ports.

Operation

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 18.

Port

Displays the port number.

GVRP active

Activates/deactivates the port *GVRP* participation.

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

[Switching > 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
- DiffServ

5.7.1 QoS/Priority Global

[Switching > 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

[Switching > 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 18.

Port

Displays the port number.

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 forwards 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 forwards 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 forwards 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 forwards 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 forwards 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

[Switching > QoS/Priority > 802.1D/p Mapping]

The device forwards 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 18.

VLAN priority

Displays the VLAN priority.

Traffic class

Specifies the *traffic class* assigned to the VLAN priority.

Possible values:

- `0..7`
  `0` assigned to the priority queue with the lowest priority.
  `7` assigned to the priority queue with the highest priority.

Note:
Among other things redundancy mechanisms use the highest *traffic class*. Therefore, select another *traffic class* for application data.

Default assignment of the VLAN priority to traffic classes

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
`0`	2	`Best Effort` Normal data without prioritizing
`1`	0	`Background` Non-time-sensitive data and background services
`2`	1	`Standard` Normal data
`3`	3	`Excellent Effort` Crucial data
`4`	4	`Controlled Load` Time-sensitive data with a high priority

VLAN Priority	Traffic class	Content description according to IEEE 802.1D
5	5	Video Video transmission with delays and jitter <100 ms
6	6	Voice Voice transmission with delays and jitter <10 ms
7	7	Network Control Data for network management and redundancy mechanisms

5.7.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

The device forwards 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 18.

DSCP value

Displays the DSCP value.

Traffic class

Specifies the *traffic class* which is assigned to the DSCP value.

Possible values:

- `0..7`
  `0` assigned to the priority queue with the lowest priority.
  `7` assigned to the priority queue with the highest priority.

Default assignment of the DSCP values to traffic classes

DSCP Value	DSCP Name	Traffic class
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5

DSCP Value	DSCP Name	Traffic class
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.7.5 Queue Management

[Switching > QoS/Priority > 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*.

You also have the option of assigning a minimum bandwidths to every *traffic classes* which the device uses to process the priority queues with *Weighted Fair Queuing*.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Traffic class

Displays the *traffic class*.

Strict priority

Activates/deactivates the processing of the port priority queue with *Strict priority* for this *traffic class*.

Possible values:

- `marked` (default setting)
  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.
- `unmarked`
  The processing of the port priority queue with *Strict priority* is inactive. The device uses *Weighted Fair Queuing*/"Weighted Round Robin" (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.

Min. bandwidth [%]

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:

- `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 %.

Max. bandwidth [%]

Specifies the shaping rate at which a *traffic class* transmits packets (Queue Shaping).

Possible values:

- `0` (default setting)
  The device does not reserve any bandwidth for this *traffic class*.
- `1..100`
  The device reserves the specified bandwidth for this *traffic class*. The specified value in percent refers to the maximum available bandwidth on this port.

For example, using Queue Shaping lets you limit the rate of a strict high-priority queue. Limiting a strict high-priority queue lets the device also process low-priority queues. To use queue shaping, you set the maximum bandwidth for a particular queue.

5.7.6 DiffServ

[Switching > QoS/Priority > DiffServ]

Differentiated Services (DiffServ) filter data packets to prioritize or limit the data stream.
- In a class, you specify the filter criteria.
- In a policy, you link the class with actions.

The device applies the actions of the policy to those data packets that meet the filter criteria of the assigned class.

To set up DiffServ, perform the following steps:
- ☐ Create a class with the filter criteria.
- ☐ Create a policy.
- ☐ Assign a class with the filter criteria to the policy.
- ☐ Specify the actions of the policy.
- ☐ Assign the policy to a port.
- ☐ Activate the DiffServ function.

The device lets you use the following per class and per instance configurations:
- 13 rules per class
- 28 instances per policy
- 3 attributes per instance

The menu contains the following dialogs:

- DiffServ Overview
- DiffServ Global
- DiffServ Class
- DiffServ Policy
- DiffServ Assignment

5.7.6.1 DiffServ Overview

[Switching > QoS/Priority > DiffServ > Overview]

This dialog displays the DiffServ settings used in the device.

Overview

The top level displays:

- The ports for which someone has set up a DiffServ policy.
- The direction of the data packets which the DiffServ policy affects.

The subordinate levels display:

- The *Policy name* string and the *Policy index* number.
- The *Policy instance* number.
- The *Class name* string and the *Protocol* name.
- The settings specified in the DiffServ class.

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.



Expands the levels. The overview then displays every level of the items.

To collapse the levels again, click the  button. The overview then displays only the first 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.

5.7.6.2 DiffServ Global

[Switching > QoS/Priority > DiffServ > Global]

In this dialog, you enable the DiffServ function.

Operation

Operation

Enables/disables the *DiffServ* function.

Possible values:

- *On*
  The *DiffServ* function is enabled.
  The device processes data packets according to the DiffServ rules.
- *Off* (default setting)
  The *DiffServ* function is disabled.

5.7.6.3 DiffServ Class

[Switching > QoS/Priority > DiffServ > Class]

In this dialog, you specify the data packets to which the device executes the actions specified in the *Switching > QoS/Priority > DiffServ > Policy* dialog. This assignment is called a class.

Only one class can be assigned to a policy. This means each class can contain multiple filter criteria.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row. See “[Create window]” on page 295.


Remove

Removes the selected table row.

Class name

Specifies the name of the DiffServ class. The device lets you change the class name directly in the table.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Criteria

Displays the specified criteria for this rule.

[Create window]

Class name

Specifies the name of the DiffServ class.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Type

Specifies the type of Class Rule for matching; this determines the individual match conditions for the present class rule.

Depending on which value you select, the following visible parameters change.

To match every packet regardless of content, select the value *every*.

Possible values:

- *cos* (default setting)
- *dstip*
- *dstl4port*
- *dstmac*
- *every*
- *ipdscp*
- *ipprecedence*
- *iptos*
- *protocol*
- *refclass*
- *srcip*
- *srcl4port*
- *srcmac*
- *cos2*
- *etype*
- *vlanid*
- *vlanid2*

Type = cos

COS

Specifies the *Class of Service* value as the match value for the class.

Possible values:

- `0..7` (default setting: `0`)

Type = dstip

Destination IP address

Specifies the destination IP address as the match value for the class.

Possible values:

- Valid IP address

Destination IP address mask

Specifies the mask for the destination IP address.

Possible values:

- Valid netmask

Type = dstl4port

Destination port

Specifies the destination Layer 4 port as the match value for the class.

Possible values:

- Valid TCP or UDP port number

Type = dstmac

Destination MAC address

Specifies the destination MAC address as the match value for the class.

Possible values:

- Valid MAC address

Destination MAC address mask

Specifies the mask for the destination MAC address.

Possible values:

- Valid netmask

Type = ipdscp

DSCP

Specifies the *DSCP (Differentiated Services Code Point)* value as the match value for the class.

Possible values:

- `0..63` (default setting: `0(be/cs0)`)

`Type = ipprecedence`

TOS priority

Specifies the *IP Precedence* value as the match value for the class. The bits are the high-order 3 bits of the *Service Type* octet in the IPv4 header.

Possible values:

- `0..7` (default setting: `0`)

`Type = iptos`

TOS mask

Specifies the IP TOS bits and mask as the match value for the class. The TOS bits are the 8 bits of the *Service Type* octet in the IPv4 header.

Possible values:

- `0x00..0xFF`

`Type = protocol`

Protocol number

Specifies the value of the *Protocol* field in the IPv4 header as the match value for the class.

Possible values:

- `0..255`
  Some common values are listed here:
  - `1`
    ICMP
  - `2`
    IGMP
  - `4`
    IPv4 (IPv4 in IPv4 encapsulation)
  - `6`
    TCP
  - `17`
    UDP
  - `41`
    IPv6 (IPv6 in IPv4 encapsulation)
  - `255`
    A rule with this value matches every protocol in the list.

The IANA defined the “Assigned Internet Protocol Numbers” that you enter here.

To find a list of the assigned numbers use the following link: www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

Type = refclass

Ref class

Specifies the parent class as a corresponding reference class. This reference class uses the set of match rules specified in a parent class as the match value.

Possible values:

- <Name of the DiffServ Class>

Conditions:

- If the reference class refers only to the parent class, then the parent class to which you bind this rule and the reference class produce the same results.
- Any attempt to delete the parent class while still referenced to by another class fails.
- If the reference class uses the parent class as the match value, then any subsequent change to the parent class rules changes the reference class rules only.
- You add subsequent rules to the parent class compatible with the rules existing in the reference class.

Type = srcip

Source IP address

Specifies the source IP address as the match value for the class.

Possible values:
- Valid IP address

Source IP address mask

Specifies the mask for the source IP address.

Possible values:
- Valid netmask

Type = srcl4port

Source port

Specifies the source Layer 4 port as the match value for the class.

Possible values:
- Valid TCP or UDP port number

Type = srcmac

Source MAC address

Specifies the source MAC address as the match value for the class.

Possible values:
- Valid MAC address and mask

Source MAC address mask

Specifies the mask for the source MAC address.

Possible values:
- Valid netmask

Type = cos2

COS 2

Specifies a secondary *Class of Service* value as the match value for the class.

Possible values:
- `0..7` (default setting: `0`)

Type = etype

Etype

Specifies the *Ethertype* value as the match value for the class.

Possible values:

- *custom* (default setting)
  You specify the Ethertype in the *Etype value* field.
- *appletalk*
- *arp*
- *ibmsna*
- *ipv4*
- *ipv6*
- *ipx*
- *mplsmcast*
- *mplsucast*
- *netbios*
- *novell*
- *pppoe*
- *rarp*

Etype value

Specifies the user-defined Ethertype value.

The prerequisite is that in the *Etype* field the value *custom* is specified.

Possible values:

- 0x0600..0xFFFF

Type = vlanid

VLAN ID

Specifies the VLAN ID as the match value for the class.

Possible values:

- 1..4042

Type = vlanid2

VLAN2 ID

Specifies the secondary VLAN ID as the match value for the class.

Possible values:

- 1..4042

5.7.6.4 DiffServ Policy

[Switching > QoS/Priority > DiffServ > Policy]

In this dialog, you specify which actions the device performs on data packets which fulfill the filter criteria specified in the *Switching > QoS/Priority > DiffServ > Class* dialog. This assignment is called a policy.

Only one policy can be assigned to a port. Each policy can contain multiple actions.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row. See “[Create window]” on page 302.


Remove

Removes the selected table row.


Modify attribute

Opens the *Modify attribute* window to specify the action that the device performs on the data packets. The prerequisite is that the table row that contains a value in the *Attribute* column is selected.

Policy name

Displays the name of the policy.

To change the value, click the relevant field.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Direction

Displays the data packets (receiving or sending) to which the device applies the policy.

Possible values:

- *in*
  The device applies the policy to the data packets that it receives.
- *out*
  The device applies the policy to the data packets that it sends.

Class name

Displays the name of the class that is assigned to the policy.

The filter criteria are specified in the class.

Attribute

Displays the action that the device performs on the data packets.

- To change an existing action, select the affected table row and click the button.
- To add further actions to a policy, click the button.

[Create window]

In this dialog, you add a policy or add further actions to an existing policy.

Policy name

Specifies the name of the policy.

- To add a policy, enter a new name.
- To add more actions to an existing policy, select a name in the list.

Possible values:

- Alphanumeric ASCII character string with 1..31 characters

Direction

Specifies the data packets (receiving or sending) to which the device applies the policy.

Possible values:

- *in* (default setting)
  The device applies the policy to the data packets that it receives.
- *out*
  The device applies the policy to the data packets that it sends.

Class name

Assigns the class to the policy.

The filter criteria are specified in the class.

Type

Specifies the policy type.

Depending on which value you select, the following visible parameters change.

Possible values:

- *markCosVal* (default setting)
- *markIpDscpVal*
- *markIpPrecedenceVal*

- *policeSimple*
- *policeTworate*
- *assignQueue*
- *drop*
- *redirect*
- *mirror*
- *markCosAsSecCos*

Type = markCosVal

Overwrites the priority field in the VLAN tag of the Ethernet packets:

- In the VLAN tag, the device overwrites the priority value in the *COS* parameter.
- With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
- With data packets without VLAN tags, the device adds a priority tag.

Can be combined with *Type* = *redirect* and *mirror*.

COS

Specifies the priority value that the device writes to the priority field of the VLAN tag of the Ethernet packets.

Possible values:

▶ 0..7

Type = markIpDscpVal

Overwrites the DS field of the IP packets.

The device writes the value specified in the *DSCP* parameter to the DS field. Subsequent devices in the network to which the device forwards the IP packets, prioritize the IP packets according to this setting. For making the device prioritize the IP packets, also enqueue the IP packets with *Type* = *assignQueue* into the desired queue.

Can be combined with *Type* = *assignQueue*, *redirect*, and *mirror*.

DSCP

Specifies the value that the device writes to the DS field of the IP packets.

Possible values:

▶ 0..63

Type = markIpPrecedenceVal

Overwrites the TOS field of the IP packets.

The device writes the value specified in the *TOS priority* parameter to the TOS field.

Can be combined with *Type* = *assignQueue*, *redirect*, and *mirror*.

TOS priority

Specifies the value that the device writes to the TOS field of the IP packets.

Possible values:

▶ 0..7

Type = policeSimple

Limits the classified data stream to the values specified in the *Simple C rate* and *Simple C burst* fields:

- If the transfer rate and burst size of the data stream are below the specified values, then the

device applies the action specified in the *Conform action* field.

- If the transfer rate and burst size of the data stream are above the specified values, then the device applies the action specified in the *Non conform action* field.

Can be combined with *Type* = `assignQueue`, `redirect`, and `mirror`.

Simple C rate

Specifies the committed rate in kbit/s.

Upper limit

Possible values:

- `1..4294967295 (2³²-1)`

Simple C burst

Specifies the committed burst size in kBytes.

Possible values:

- `0..128`

Conform action, Non conform action

In the *Conform action* field, you specify the action that the device applies to the compliant data stream. Compliant means that the data stream is under the limits specified in the parameters *Simple C rate* and *Simple C burst*.

In the *Non conform action* field, you specify the action that the device applies to the non-compliant data stream. Non-compliant means that the data stream is over the limits specified in the parameters *Simple C rate* and *Simple C burst*.

Possible values:

- *drop*
  Discards the data packets.
- *markDscp*
  Overwrites the DS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..63`] to the DS field.
- *markPrec*
  Overwrites the TOS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..7`] to the TOS field.
- *send*
  Sends the data packets.
- *markCos*
  Overwrites the priority field in the VLAN tag of the Ethernet packets:
  - in the VLAN tag, the device overwrites the priority value in the *COS* parameter.
  - With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
  - With Ethernet packets without VLAN tags, the device adds a priority tag.

- *markCos2*
  With QinQ-tagged Ethernet packets, overwrites the priority field in the inner tag (*Customer tag* or *C tag*) with the value specified in the adjacent field [0..7].
- *markCosAsSecCos*
  Overwrites the priority field in the outer tag (*Service tag* or *S tag*) with the priority value of the inner tag (*C tag*).

Color conform class

Specifies the class of the received data stream that the devices designates as conform (green).

Possible values:

- *blind*
  The device operates in the *Color-Blind* mode. The devices designates the complete data stream received as conform (green).
- <Name of the DiffServ Class>
  The devices designates only this class of the received data stream as conform (green). Those classes are selectable for which in the *Switching > QoS/Priority > DiffServ > Class* dialog, *Criteria* column a rule of the type *cos*, *ipdscp*, *ipprec*, *cos2* is specified.

Verify that the filter criteria of the class selected from the *Class name* drop-down list above and of the class selected from this drop-down list, is neither identical nor exclude each other. Exclusion criteria are:

- The filter criteria have the same rule type, for example *cos* and *cos*. Use classes with a different rule type, for example *cos* and *ipdscp*.
- One of the classes references with the rule type *refclass* another class that conflicts with the used classes.

Type = policeTworate

Limits the classified data stream to the values specified in the *Two rate C rate*, *Two rate C burst*, *Two rate P rate*, and *Two rate P burst* fields.

- If the transfer rate and burst size are below *Two rate C rate* and *Two rate C burst*, then the device applies the *Conform action* action to the data stream.
- If the transfer rate and burst size are between *Two rate C rate* and *Two rate P rate* as well as *Two rate C burst* and *Two rate P burst*, then the device applies the *Exceed action* action to the data stream.
- If the transfer rate and burst size are above *Two rate P rate* and *Two rate P burst*, then the device applies the *Non conform action* action to the data stream.

Can be combined with *Type* = *assignQueue*, *redirect*, and *mirror*.

Two rate C rate

Specifies the committed rate in kbit/s.

Possible values:

▶ 1..4294967295 (2^{32}-1)

Two rate C burst

Specifies the committed burst size in kBytes.

Possible values:

▶ 0..128

Two rate P rate

Specifies the peak rate (max. allowable transfer rate of the data stream) in kbit/s.

Possible values:

▶ 1..4294967295 (2^{32}-1)

Two rate P burst

Specifies the peak burst size (max. allowable burst size) in kBytes.

Possible values:

▶ 1..128

Conform action
Conform value
Exceed action
Exceed value
Non conform action
Non conform value

In the *Conform action* field, you specify the action that the device applies to the compliant data stream. Compliant means that transfer rate and burst size are below *Two rate C rate* and *Two rate C burst*.

In the *Exceed action* field, you specify the action that the device applies to the data stream. The prerequisite is that the transfer rate and burst size are between *Two rate C rate* and *Two rate P rate*

as well as *Two rate C burst* and *Two rate P burst*.

In the *Non conform action* field, you specify the action that the device applies to the non-compliant data stream. Non-compliant means that the transfer rate and burst size are above *Two rate P rate* and *Two rate P burst*.

Possible values:

- `drop`
  Discards the data packets.
- `markDscp`
  Overwrites the DS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..63`] to the DS field.
- `markPrec`
  Overwrites the TOS field of the IP packets.
  The device writes the value specified in the adjacent field [`0..7`] to the TOS field.
- `send`
  Sends the data packets.
- `markCos`
  Overwrites the priority field in the VLAN tag of the Ethernet packets:
  - in the VLAN tag, the device overwrites the priority value in the *COS* parameter.
  - With QinQ-tagged (IEEE 802.1ad) Ethernet packets, the device writes the value to the outer tag (*Service tag* or *S tag*).
  - With Ethernet packets without VLAN tags, the device adds a priority tag.
- `markCos2`
  With QinQ-tagged Ethernet packets, overwrites the priority field in the inner tag (*Customer tag* or *C tag*) with the value specified in the adjacent field [`0..7`].
- `markCosAsSecCos`
  Overwrites the priority field in the outer tag (*S tag*) with the priority value of the inner tag (*C tag*).

Color conform class

Specifies the class of the received data stream that the devices designates as conform (green).

Possible values:

- `0 - blind`
  The device operates in the *Color-Blind* mode. The devices designates the complete data stream received as conform (green).
- `<Name of the DiffServ Class>`
  The devices designates only this class of the received data stream as conform (green).
  Those classes are selectable for which in the *Switching > QoS/Priority > DiffServ > Class* dialog, *Criteria* column a rule of the type `cos`, `ipdscp`, `ipprec`, `cos2` is specified.

Verify that the filter criteria of the class selected from the *Class name* drop-down list above and of the class selected from this drop-down list, is neither identical nor exclude each other. Exclusion criteria are:

- The filter criteria have the same rule type, for example `cos` and `cos`. Use classes with a different rule type, for example `cos` and `ipdscp`.
- One of the classes references with the rule type `refclass` another class that conflicts with the used classes.

Type = assignQueue

Changes the priority queue into which the device adds the data packets.

The device enqueues the data packets into the priority queue with the ID specified in the *Queue ID* parameter.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *drop*, *markCosVal*, and *markCosAsSecCos*.

Queue ID

Specifies the ID of the priority queue into which the device adds the data packets. See the *Traffic class* field in the *Switching > QoS/Priority > 802.1D/p Mapping* dialog.

Possible values:

- `0..7`

Type = drop

Discards the data packets.

Can be combined with *Type* = *mirror*, if *mirror* is set up first.

Type = redirect

The device forwards the received data stream to the port specified in the *Redirection interface* field.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *markCosVal*, *markIpDscpVal*, *markIpPrecedenceVal*, *policeSimple*, *policeTworate*, *assignQueue*, and *markCosAsSecCos*.

Redirection interface

Specifies the destination port.

Possible values:

- `<Port number>`
  Number of the destination port. The device forwards the data packets to this port.

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 superfluous data packets on the destination port.

Type = mirror

The device copies the received data stream and also transfers it to the port specified in the *Mirror interface* field.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *markCosVal*, *markIpDscpVal*, *markIpPrecedenceVal*, *policeSimple*, *policeTworate*, *assignQueue*, and *markCosAsSecCos*.

Mirror interface

Specifies the destination port.

Possible values:

- <Port number>
  Number of the destination port. The device copies the data packets to this port.

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 superfluous data packets on the destination port.

Type = markCosAsSecCos

Overrides the priority field in the outer VLAN tag of the Ethernet packets with the priority value of the inner VLAN tag.

Apply this action only to data packets that the device receives.

Can be combined with *Type* = *assignQueue*, *redirect*, and *mirror*.

5.7.6.5 DiffServ Assignment

[Switching > QoS/Priority > DiffServ > Assignment]

In this dialog, you assign the policy to a port.

Note:
You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row. See “[Create window]” on page 312.


Remove

Removes the selected table row.

Port

Displays the port number.

Direction

Displays the interface direction to which you assigned the policy.

Policy name

Displays the name of the policy assigned to the interface.

Status

Displays the port status.

Active

Activates/deactivates the DiffServ parameters associated with this table row.

Possible values:

- `marked`
  The device forwards the data packets according to the specified DiffServ settings.
- `unmarked`
  The device forwards the data packets without regarding the specified DiffServ settings.

[Create window]

Port

Specifies the port to which the table row relates.

Possible values:

- Available ports

Direction

Specifies the direction in which the device applies the policy.

Possible values:

- *In* (default setting)
- *Out*

Note:
On the port, you cannot assign an *Out* policy to a class that contains both L2 and L3 class rules, that is, a class that contains rules from both the following groups:
- *dstmac*, *srcmac*, *etype*
- *srcip*, *dstip*, *srcl4port*, *dstl4port*, *protocol*, *ipprecedence*, *iptos*, *ipdscp*
Example: If you have specified both *srcmac* and *dstip* rules for a class, you cannot assign an *Out* policy to this class.

Policy

Specifies the policy assigned to the port.

Possible values:

- Available policies

5.8 VLAN

[Switching > VLAN]

With VLAN (Virtual Local Area Network) you distribute the data packets in the physical network to logical subnets. 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 IEEE 802.1Q. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device forwards 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
- MAC-based VLAN
- IP subnet-based VLAN
- Protocol-based VLAN
- Port-based VLAN

The menu contains the following dialogs:
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice
- MAC Based VLAN
- Subnet-based VLAN
- Protocol Based VLAN

5.8.1 VLAN Global

[Switching > 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 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 set up in the device.

See the *Switching > VLAN > Configuration* dialog.

The VLAN 1 is permanently set up in the device.

Double VLAN tag ethertype

Displays the value of the outer VLAN tag that a *Core* port adds to the data packet to be forwarded.

Possible values:

- `0x8100 (802.1Q)`
  Normal VLAN tag

5.8.2 VLAN Configuration

[Switching > VLAN > Configuration]

In this dialog, you manage the VLANs. To set up a VLAN, add 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 sets up dynamic VLANs:
  - *MRP*: If you assign to the ring ports a non-existing VLAN, then the device sets up this VLAN.
  - *MVRP*: The device sets up 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 18.

Buttons


Add

Opens the *Create* window to add a table row.

In the *VLAN ID* field, you specify the VLAN ID.


Remove

Removes the selected table row.

VLAN ID

ID of the VLAN.

The device supports up to 512 VLANs simultaneously set up.

Possible values:

- `1..4042`

Status

Displays how the VLAN is set up.

Possible values:

- *other*
  VLAN `1`
  or
  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.

Name

Specifies the name of the VLAN.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

RSPAN VLAN

Specifies the VLAN as the RSPAN VLAN.

Possible values:

- `marked`
  The device uses the VLAN exclusively to send the RSPAN data packets in the direction of the *Destination port* of the *Destination switch*. See the *Diagnostics > Ports > RSPAN* dialog. Do not use the VLAN for any other purposes.
  The device disables source MAC address learning in the VLAN.
- `unmarked` (default setting)
  The device does not use the VLAN to send RSPAN data packets.

<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 has automatically set up the entry 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.
- `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 has automatically set up the entry 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, connections to the device management interrupt when you apply the changes. Then, access to the device management is only possible using the Command Line Interface through the serial connection.

5.8.3 VLAN Port

[Switching > 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 forwards 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 ID in the tag 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 18.

Port

Displays the port number.

Port-VLAN ID

Specifies the VLAN ID which the device assigns to data packets received without a VLAN tag.

Prerequisites:
- In the *Acceptable packet types* column, the value `admitAll` is specified.

Possible values:
- `1..4042` (default setting: `1`)
  A VLAN you set up.

If you use the *MRP* function and you did not assign a VLAN to the ring ports, then 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 port is a member. See the *Switching > VLAN > Configuration* dialog. If the VLAN ID in the data packet matches one of these VLANs, then the device forwards the data packet. Otherwise, the device discards the data packet.
- `unmarked` (default setting)
  The ingress filtering is inactive.
  The device forwards received data packets without comparing the VLAN ID. Thus, the device also forwards data packets in VLANs in which the port is not a member.

Double VLAN tag mode

Activates/deactivates the *Double VLAN Tag mode* on the port.

Possible values:

- `marked`
  The *Double VLAN Tag mode* is active on the port.
  The port operates as a *Core* port. The device adds an outer VLAN tag to the data packet to be forwarded on the port. The *Ethertype* value of this VLAN tag you specify in the *Switching > VLAN > Global* dialog.
- `unmarked` (default setting)
  The *Double VLAN Tag mode* is inactive on the port.
  - If the checkbox is unmarked for each other port, then the port operates as a normal port.
  - If the checkbox is marked for any other port, then the port operates as an *Access* port. The device assigns the *Port-VLAN ID* value of the port to each received data packet. The port forwards the originally received data packet with or without a VLAN tag.

The port VLAN ID is the tunnel VLAN ID. You add the port as a member to the appropriate VLAN. The port transmits the data packets without a VLAN tag.

5.8.4 VLAN Voice

[Switching > 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 set-up Voice VLAN. The member set is either tagged or untagged. Tagging depends on the Voice VLAN interface mode (*vlan*, *dot1p-priority*, *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 packets with VLAN tag, priority tag or untagged. This depends on the specified Voice VLAN Interface mode. You activate Voice VLAN on the port which is connecting to the VoIP phone.

Operation

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 18.

Port

Displays the port number.

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.

- *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 using the same cable for transmitting data.

Possible values:

- `marked` (default setting)
  If voice data packets are present on the interface, then the data packets have the normal priority.
- `unmarked`
  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 VLAN ID to which the table row relates. To forward data packets to this VLAN using this filter, select in the *Voice VLAN mode* column the value *vlan*.

Possible values:

- `1..4042` (default setting: `0`)

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)..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`

5.8.5 MAC Based VLAN

[Switching > VLAN > MAC Based VLAN]

In a MAC-based VLAN, the device forwards the data packets based on the source MAC address associated with a VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

MAC-based VLANs specify the filtering criteria only for untagged or priority-tagged packets. Assign a port to a MAC-based VLAN to transmit packets with a specific source MAC address in that VLAN. The device then forwards untagged packets received with the specified MAC address to the assigned MAC-based VLAN. Other untagged packets are subject to normal VLAN classification rules.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row.

- In the *MAC address* field, you specify the MAC address.
- In the *VLAN ID* field, you specify the VLAN ID.


Remove

Removes the selected table row.

MAC address

Displays the MAC address to which the table row relates.

The device supports up to 256 simultaneous MAC-based VLAN assignments.

Possible values:

▶ Valid MAC address

VLAN ID

Displays the ID of the VLAN to which the table row relates.

Possible values:

▶ `1..4042` (set up VLAN IDs)

5.8.6 Subnet-based VLAN

[Switching > VLAN > Subnet-based VLAN]

In IP subnet-based VLANs, the device forwards the data packets based on the source IP address and subnet mask associated with the VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

IP subnet-based VLANs specify the filtering criteria only for untagged packets or priority tagged packets. Assign a port to an IP subnet-based VLAN to transmit packets with a specific source IP address in that VLAN. The device then forwards untagged packets received with the specified IP address to the assigned IP subnet-based VLAN.

To set up an IP subnet-based VLAN, specify an IP address, a subnet mask, and the corresponding VLAN identifier. When multiple entries apply, the device uses the entry with the longest prefix first.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons



Add

Opens the *Create* window to add a table row.

- In the *IP address* field, you specify the IP address.
- In the *Netmask* field, you specify the netmask.
- In the *VLAN ID* field, you specify the VLAN ID.



Remove

Removes the selected table row.

IP address

Displays the IP address to which you assign the subnet-based VLAN.

The device supports up to 256 VLANs set up simultaneously to subnet-based VLANs.

Possible values:

- Valid IP address

Netmask

Displays the netmask to which you assign the subnet-based VLAN.

Possible values:

- Valid IP netmask

VLAN ID

Displays the VLAN ID.

Possible values:

- `1..4042`

5.8.7 Protocol Based VLAN

[Switching > VLAN > Protocol Based VLAN]

In a protocol-based VLAN, specified ports bridge data packets based on the L3 protocol (Ethertype) associated with the VLAN. User-defined packet filters determine if a packet belongs to a particular VLAN.

Protocol-based VLANs specify the filtering criteria only for untagged packets. Assign a port to a protocol-based VLAN for a specific protocol. The device then forwards untagged packets received with the specified protocol to the protocol-based VLAN. The device assigns other untagged packets with the port VLAN ID.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Group ID

Displays the group identifier of the protocol-based VLAN entry.

The device supports up to 128 protocol-based VLAN associations simultaneously.

Possible values:

- `1..128`

Name

Specifies the group name of the protocol-based VLAN entry.

Possible values:

- Alphanumeric ASCII character string with 1..16 characters

VLAN ID

Specifies the VLAN.

Possible values:

- `1..4042` (default setting: `0`)

Port

Specifies the ports that are assigned to the group.

Possible values:

- `<Port number>` (default setting: `-`)
  From the drop-down list, select the ports.

Ethertype

Specifies the Ethertype value assigned to the VLAN.

The Ethertype is a two-octet field in an Ethernet packet to indicate which protocol the payload contains.

Possible values:

- `0x0600..0xFFFF`
  Ethertype as a hexadecimal number sequence
  When you enter a decimal value, the device converts the value into a hexadecimal number sequence when you click the  button.
- `ip`
  Ethertype keyword for IPv4 (equivalent to `0x0800`)
- `arp`
  Ethertype keyword for ARP (equivalent to `0x0806`)
- `ipx`
  Ethertype keyword for IPX (equivalent to `0x8137`)

5.9 L2-Redundancy

[Switching > L2-Redundancy]

The menu contains the following dialogs:

- MRP
- HIPER Ring

- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

5.9.1 MRP

[Switching > L2-Redundancy > 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 Media Redundancy Protocol (MRP) according to IEC 62439.

If a section is not operating, then the ring structure of an MRP Ring changes back into a line structure. You can specify the maximum recovery time.

The *Ring Manager* 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* function for the ports connected to the MRP Ring. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

When you work with oversized Ethernet packets (the value in the *MTU* column for the port is >1518, see the *Basic Settings > Port* dialog), the switching time of the MRP Ring reconfiguration depends on the following parameters:
- Bandwidth of the ring line
- Size of the Ethernet packets
- Number of devices in the ring

Set the recovery time sufficiently large to help avoid delays in the MRP packages due to latencies in the devices. You can find the formula for calculating the switching time in IEC 62439-2, section 9.5.

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 set up the parameters for the MRP Ring, enable the function here.

Possible values:

- *On*
  The *MRP* function is enabled.
  After you set up 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 port that operates as a ring port.

Possible values:

- `<Port number>`

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* device 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* device 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 activate this function.

Possible values:

- *On*
  The *Ring manager* function is enabled.
  The device operates in the *Ring Manager* mode.
  To help avoid unexpected behavior, do not enable the function on a device on which the *RCP* function is enabled.
- *Off* (default setting)
  The *Ring manager* function is disabled.
  The device operates exclusively in the *Ring Client* mode.

Domain name

Specifies the name of the MRP domain that the device belongs to.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters
  You can specify any name. By entering a descriptive name, you can simplify the administration of MRP domains.

Ring recovery

Specifies the maximum recovery time in milliseconds for reconfiguration of the ring. This setting is effective only if the device operates in the *Ring Manager* mode.

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.

When you are working with oversized Ethernet packets, the number of devices in the ring is limited. Note that the switching time depends on several parameters. See the description above.

VLAN ID

Specifies the VLAN ID which you assign to the ring ports.

Possible values:

- `0` (default setting)
  No VLAN assigned.
  In the *Switching > VLAN > Configuration* dialog, assign for VLAN `1` the value `U` to the ring ports.
- `1..4042`
  VLAN assigned.
  If you assign a non-existing VLAN to the ring ports, then the device automatically sets up this VLAN. In the *Switching > VLAN > Configuration* dialog, the device adds a table row for the VLAN and assigns the value `T` to the ring ports.

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.

Domain ID

Displays a sequence of 16-bytes in decimal notation, which identifies the MRP domain that the device belongs to.

Information

Information

Displays the status of the ring.

Possible values:

- *`Redundancy available. Ring is closed.`*
  Normal operation. The components in the ring operate as intended.
- *`Configuration error: Error on ring port link.`*
  The device has detected a link error on a ring port. Verify that the correct port is selected in the *Ring port 1* and *Ring port 2* frames.
- *`Redundancy not available. Ring is open. Check the Ring clients.`*
  The device has not detected a configuration error, but no redundancy is available.
- *`Redundancy not available. At least one ring port is disabled.`*
  At least one of the ring ports is disabled. Verify that both ring ports are enabled. See the *Basic Settings > Port* dialog.
- *`Configuration error: Packets from another ring manager received.`*
  Another device exists in the ring that operates in the *Ring Manager* mode.
  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 of the ring ports.

Last time the ring was open

Displays the date and time at which the device last detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.

Number of times the ring was open

Displays the number of times the device has detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.

5.9.2 HIPER Ring

[Switching > L2-Redundancy > HIPER Ring]

The concept of HIPER Ring redundancy enables the construction of high-availability, ring-shaped networks. The device operates exclusively in the *Ring Client* mode. This function lets you extend an existing HIPER Ring or to replace a device already participating as a *Ring Client* in a HIPER Ring.

A HIPER Ring contains a *Ring Manager (RM)* device which controls the ring. The *Ring Manager* device sends watchdog packets into the ring on both the primary and secondary ports. When the *Ring Manager* device receives the watchdog packets on both ports, the *Primary port* remains in the `forwarding` state and the secondary port remains in the `discarding` state.

The device operates exclusively in the *Ring Client* mode. This means that the device detects watchdog packets on its ring ports and sends a *Link Down* or *Link Up* packet to the *Ring Manager* device when the link status changes.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, the device only supports HIPER Ring in VLAN `1`.

Note:
Spanning Tree and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* function for the ports connected to the HIPER Ring. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

Note:
Set up the devices of the HIPER Ring individually. Before you connect the redundant link, complete the setup of every device of the HIPER Ring. You thus help avoid loops during the configuration phase.

Operation

Operation

Enables/disables the *HIPER Ring* client.

Possible values:

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

Ring port 1/Ring port 2

Port

Specifies the port number of the primary/secondary ring port.

Possible values:

- `-` (default setting)
  No primary/secondary ring port selected.
- `<Port number>`
  Number of the ring port

State

Displays the state of the primary/secondary ring port.

Possible values:

- *`not-available`*
  The *HIPER Ring* client is disabled.
  or
  No primary or secondary ring port selected.
- *`active`*
  The ring port is enabled and logically up.
- *`inactive`*
  No link available on the ring port.
  As soon as the link on a ring port is interrupted, the device sends a *Link Down* packet to the *Ring Manager* device on the other ring port.

Information

Mode

Displays that the device operates in the *Ring Client* mode.

5.9.3 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

The Spanning Tree Protocol (STP) is a protocol that deactivates redundant paths of a network to help avoid loops. If a network component becomes inoperable 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.

The device supports the Multiple Spanning Tree Protocol (MSTP) standardized in IEEE 802.1, which is a further development of the Spanning Tree Protocol (STP).

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 MSTP
- Spanning Tree Port

5.9.3.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

In this dialog, you enable/disable the *Spanning Tree* function and specify the bridge settings.

Operation

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

Variant

Specifies the protocol used for the *Spanning Tree* function:

Possible values:

- *rstp* (default setting)
  The protocol RSTP is active.
  With RSTP (IEEE 802.1Q-2005), the *Spanning Tree* function operates for the underlying physical layer.
- *mstp*
  The protocol MSTP is active.
  To help avoid longer recovery times, specify the maximum value 40 in the *Tx holds* field.

Traps

Send trap

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.

Ring only mode

Active

Activates/deactivates the *Ring only mode* function, in which the device does not verify the age of the BPDUs.

Possible values:

- `marked`
  The *Ring only mode* function is active. Use this setting for applications for RSTP rings with diameters greater than 40.
- `unmarked` (default setting)
  The *Ring only mode* function is inactive.

First port

Specifies the port number of the first interface.

Possible values:

- `<Port number>` (default setting: `-`)

Second port

Specifies the port number of the second interface.

Possible values:

- `<Port number>` (default setting: `-`)

Bridge configuration

Bridge ID

Displays the *Bridge Identifier* of the device.

The device with the numerically lowest *Bridge Identifier* 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 (2¹⁵)`)

To make this device the *Root bridge*, assign the numerically lowest value for the priority 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 that the *Root bridge* specifies. 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 that the *Root bridge* specifies. See the *Root information* frame.

In the Rapid Spanning Tree Protocol (RSTP), the bridges negotiate a status change without a specified delay.

The *Spanning Tree* function 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, namely 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 that the *Root bridge* specifies. See the *Root information* frame.

The *Spanning Tree* function 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`)
  To help avoid longer recovery times when using the `MSTP` protocol, set the maximum value to `40`.

When the device sends a BPDU, the device increments a counter on this port.

When the counter reaches the value specified here, 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 the 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:
  - ☐ 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. As an alternative, 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 Identifier* 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 Rapid Spanning Tree Protocol (RSTP), the bridges negotiate a status change without a specified delay.

The *Spanning Tree* function 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, namely the number of devices to the *Root bridge*.

Possible values:

- `6..40` (default setting: `20`)

The *Spanning Tree* function 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 (2× 10⁸)`

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>`

5.9.3.2 Spanning Tree MSTP

[Switching > L2-Redundancy > Spanning Tree > MSTP]

In this dialog, you manage the settings of the global and local MST instances.

In contrast to the local MST instances, the global MST instance is set up permanently in the device. The global MST instance contains the VLANs that are not explicitly allocated to a local MST instance.

The device supports up to 31 local MST instances. To add a local MST instance, click the button.

While STP has a single Spanning Tree spanning the network, MSTP lets you set up one Spanning Tree per VLAN or group of VLANs. Thus it is possible to specify several smaller Spanning Trees covering one network.

How to help avoid longer convergence times:
- ☐ Only use devices in the network that support RSTP or MSTP.
- ☐ Adjust the following parameters to the topology and number of bridges:
  - Maximum allowed number of devices to the *Root bridge*
    Switching > L2-Redundancy > Spanning Tree > Global dialog, *Max age* field
  - Maximum allowed number of bridges within the MST region in a branch to the *Root bridge*
    Switching > L2-Redundancy > Spanning Tree > MSTP dialog, *Global CIST parameter* frame, *Hops (max.)* field

For bridges in an MST region, specify identical values for the following parameters:
- *Name* of the MST region
- *Revision level* of the MST region
- Allocation of the VLANs to the MST instances
  - Include ports connecting the bridges of an MST region as members in the VLANs set up on the bridges. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection interruptions within the MST region when the topology is changed.
  - Include ports connecting an MST region with other MST regions or with the CST region (boundary ports) as members in the VLANs set up in both regions. The ports are to transmit the data packets with a VLAN tag. You thus help avoid potential connection interruptions when topology changes affecting the boundary ports are made.

MST region identifier

Name

Specifies the name of the MST region to which the device belongs.

Possible values:

- Alphanumeric ASCII character string with 1..32 characters

Revision level

Specifies the version number of the MST region to which the device belongs.

Possible values:

- `0..65535 (2¹⁶-1)` (default setting: `1`)

Checksum

Displays the MD5 checksum of the MST configuration.

Global CIST parameter

Hops (max.)

Specifies the maximum number of bridges within the MST region in a branch to the *Root bridge*.

Possible values:

- `6..40` (default setting: `20`)

Attached VLANs

Displays the IDs of the VLANs that are assigned only to the global MST instance and to no other local MST instance.

Possible values:

- `ID of the statically configured VLANs`
  (default setting: `1`)

Bridge ID

Displays the *Bridge Identifier* of the device.

Possible values:

- `<Bridge priority> / <MAC address>`
  The value is made up as follows:
  - Value in the *Priority* field. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog, *Bridge configuration* frame.
  - MAC address of the device.

Root ID

Displays the *Bridge Identifier* of the current *CIST Root bridge* of the whole Layer 2 network.

Possible values:

- `<Bridge priority> / <MAC address>`

The device with the numerically lowest *Bridge Identifier* value takes over the role of the *CIST Root bridge* in the network. The following devices are able to take over the role of the *Root bridge*:

- Bridges not belonging to any MST region
- Bridges belonging to the global instance of an MST region

In the whole Layer 2 network, the bridges use the time settings of the *CIST Root bridge*, for example *Hello time [s]*.

Regional root ID

Displays the *Bridge Identifier* of the current *Root bridge* that belongs to the global instance of the MST region to which this device belongs.

Possible values:

- `<Bridge priority> / <MAC address>`

The values in the *Regional root ID* and *Root ID* fields are identical when the regional *Root bridge* has the numerically lowest *Bridge Identifier* value in the whole Layer 2 network.

Root port

Displays the port of the device from which the path leads to the current *CIST Root bridge* of the whole Layer 2 network.

Possible values:

- `no Port`
  The device currently has the role of the *Root bridge*.
- `<Port number>`
  The path to the current *CIST Root bridge* of the whole Layer 2 network leads over this port.

Root path cost

Displays the path cost for the path that leads from the regional *Root bridge* of the MST region to the current *CIST Root bridge* of the whole Layer 2 network.

Possible values:

- `0`
  The regional *Root bridge* simultaneously has the role of the *CIST Root bridge*.
- `1..200000000 (2× 10⁸)`
  For the devices within an MST region, the *Root path cost* values are identical.

If you do not use the *MSTP* function, then the *Root path cost* values are identical to the root path costs of STP or RSTP. In this case, every device considers itself as an own region.

Internal root path cost

Displays the internal path cost for the path that leads from the *Root port* of the device to the current regional *Root bridge* of the MST region.

Possible values:

- `0`
  The local bridge simultaneously has the role of the current regional *Root bridge*.
- `1..200000000 (2× 10⁸)`

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Adds a table row.

The device supports up to local 16 instances.

Remove

Removes the selected table row.

Configure VLANs

Opens the *Configure VLANs* window to allocate VLANs to the local MST instance which is selected in the table.

MSTI

Displays the instance number of the local MST instance.

Attached VLANs

Displays the IDs of the VLANs that are allocated to this local MST instance.

Priority

Specifies the *Bridge priority* of the local MST instance.

Possible values:

- `0..61440` in steps of 4096 (default setting: `32768 (2¹⁵)`)

Assign the numerically lowest value for the priority in this local MST instance to the device to make this device the *Root bridge*.

Bridge ID

Displays the *Bridge Identifier*.

The device with the numerically lowest *Bridge Identifier* value takes over the role of the regional MSTI *Root bridge* in the instance.

Possible values:

- `<Bridge priority + Number of the instance> / <MAC address>`
  Sum of the value in the *Priority* and *MSTI* fields / MAC address of the device.

Time since topology change

Displays the time that has elapsed since the last topology change within this instance.

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.

Topology change

Displays if the device has detected a topology change within the instance.

Possible values:

- `marked`
  The device has detected a topology change.
- `unmarked`
  The device has not detected a topology change.

Root ID

Displays the *Bridge Identifier* of the current *Root bridge* in this instance.

Possible values:

- `<Bridge ID> / <MAC address>`

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 instance.

Possible values:

- `0`
  The bridge is simultaneously the *Root bridge* of the instance.
- `1..200000000 (2× 10⁸)`

Root port

Displays the port of the device from which the current path leads to the *Root bridge* of the instance.

Possible values:

- `no Port`
  The device currently has the role of the *Root bridge*.
- `<Port number>`
  The path to the current *Root bridge* of the instance leads over this port.

5.9.3.3 Spanning Tree Port

[Switching > L2-Redundancy > 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]
- [MSTI <MSTI>]

[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 18.

Port

Displays the port number.

STP active

Activates/deactivates the *Spanning Tree* function on the port.

Possible values:

- `marked` (default setting)
  The *Spanning Tree* function is active on the port.
- `unmarked`
  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.

Port state

Displays the transmission status of the port.

Possible values:

- *discarding*
  The port is blocked and forwards only STP-BPDUs.

- *learning*
  The port is blocked, but it learns the MAC addresses of received data packets.
- *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.
- *master*
  Port with the cheapest path to the CIST. The port is the *CIST Root port* of the regional *CIST Root bridge*. The port is unique in an MST region.
- *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 (2× 10⁸)` (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:

- `0..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 Identifier* 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 detected 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 detected 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* in the local MST instance 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 detected 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` state without changing to the `learning` state 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` state, 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 × *Hello time [s]*, the device sets the port to the *forwarding* status (default setting 1.5 × 2 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 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.
    and/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 18.

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 the 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 the network from attacks with STP-BPDUs that try to change the topology.

Possible values:

- `marked`
  The monitoring of *Topology Change* notifications is active.
  - 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* function is active.
    Example: The device receives better path information for the *Root bridge*.
- `unmarked` (default setting)
  The monitoring of *Topology Change* notifications is inactive.
  If the device receives STP-BPDUs with a *Topology Change* flag, then the device deletes the MAC address table (forwarding database) 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:
  - ☐ 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.

[MSTI <MSTI>]

This tab lets you specify the settings on the ports for path costs and priority in the local MST instance, and to view current values.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Port state

Displays the transmission status of the port.

Possible values:

- *discarding*
  The port is blocked and forwards only STP-BPDUs.
- *learning*
  The port is blocked, but it learns the MAC addresses of received data packets.
- *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

Specifies the current role of the port in the local instance.

Possible values:

- *root*
  Port with the cheapest path to the *Root bridge*.
- *alternate*
  Port with the alternative path to the *Root bridge* (currently interrupted).
- *designated*
  Port for the side of the tree averted from the *Root bridge*.
- *backup*
  Port which receives STP-BPDUs from its own device.
- *master*
  Port with the cheapest path to the CIST. The port is the *CIST Root port* of the *CIST* Regional Root. The port is unique in an MST region.
- *disabled*
  The port is inactive. See the *Basic Settings > Port* dialog, *Configuration* tab.

Port path cost

Specifies the path costs of the port in the local instance.

Possible values:

- `0..200000000 (2× 10⁸)` (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 in the local instance.

Possible values:

- `0..240` in steps of 16 (default setting: `128`)

Received bridge ID

Displays the *Bridge Identifier* of the device from which this port last received an STP-BPDU in the local instance.

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 detected 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 detected 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.

5.9.4 Link Aggregation

[Switching > L2-Redundancy > 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 criteria for distributing the load to the parallel links are based on the *Hashing option* function.

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.

The device lets you set a maximum of 16 Link Aggregation groups.

Configuration

Hashing option

Specifies which information the device uses to distribute the packets to the physical ports of the LAG interface. The device sends packets containing the same distribution-relevant information over the same physical port to keep the packet order.

This setting overwrites the value specified in the *Hashing option* column for the port.

Possible values:

- *sourceMacVlan*
  The device uses the `Source MAC address`, `VLAN ID`, `EtherType` fields of the packet, and the physical ingress port.
- *destMacVlan*
  The device uses the `Destination MAC address`, `VLAN ID`, `EtherType` fields of the packet, and the physical ingress port.
- *sourceDestMacVlan* (default setting)
  The device uses the `Source MAC address`, `Destination MAC address`, `VLAN ID`, `EtherType` fields of the packet, and the physical ingress port.
- *sourceIPsourcePort*
  The device uses the `Source IP address` and `Source TCP/UDP port` fields of the packet.
- *destIPdestPort*
  The device uses the `Destination IP address` and `Destination TCP/UDP port` fields of the packet.
- *sourceDestIPPort*
  The device uses the `Source IP address`, `Destination IP address`, `Source TCP/UDP port`, and `Destination TCP/UDP port` fields of the packet.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 set up 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 inoperable.
- *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.
  Consider that the following protocols do not work properly on the physical ports when you activate the LAG interface:
  – *PTP*
- unmarked
  The LAG interface is inactive.

STP active

Activates/deactivates the *Spanning Tree* function 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* function on the LAG interfaces in the *Switching* > L2-Redundancy > *Spanning Tree > Port* dialog.

Possible values:

- marked (default setting)
  The *Spanning Tree* function is active on this LAG interface.
- unmarked
  The *Spanning Tree* function 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.

Hashing option

Specifies which information the device uses to distribute the packets to the individual physical ports of the LAG interface. This setting has priority over the value selected in the *Configuration* frame, *Hashing option* drop-down list.

For further information on the values, see the description of the *Hashing option* drop-down list in the *Configuration* frame.

MTU

Specifies the maximum allowed size of Ethernet packets on the LAG interface in bytes. Any present VLAN tag is not taken into account.

This setting lets you increase the size of the Ethernet packets for specific applications.

Possible values:

- `1518..12288` (default setting: `1518`)
  With the value `1518`, the LAG interface transmits the Ethernet packets up to the following size:
  - 1518 bytes without VLAN tag
    (1514 bytes + 4 bytes CRC)
  - 1522 bytes with VLAN tag
    (1518 bytes + 4 bytes CRC)

Track name

Displays the name of the tracking object made up of the values displayed in the *Type* and *Track ID* columns.

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 use this function to force the device to switch automatically to the redundant line.

Possible values:

- `1..x` (default setting: `1`)
  The maximum value depends on the number of physical ports assigned to the LAG interface.

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.
  When the device detects a link up/down status change, 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 (2¹⁶-1)`
  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 (2¹⁶-1)`
  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 LACPDU parameters.

The device lets you mix the values. From the drop-down list, select one or more items.

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 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 LACPDUs.

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 IEEE 802.1AX-2014.

5.9.5 Link Backup

[Switching > L2-Redundancy > Link Backup]

With Link Backup, you set up 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. When you activate the *Fail back* function and the *Primary port* returns to normal operation, the device first blocks the data packets on the *Backup port* and then forwards the data packets to the *Primary port*. This process helps protect the device from causing loops in the network.

Operation

Operation

Enables/disables the Link Backup function globally in the device.

Possible values:

- *On*
  Enables the Link Backup function.
- *Off* (default setting)
  Disables the Link Backup function.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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* to 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 cable is unplugged, the port is powered off, the port link is interrupted, or a function in the device has disabled the port.
- *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 cable is unplugged, the port is powered off, the port link is interrupted, or a function in the device has disabled the port.
- *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*.

5.9.6 FuseNet

[Switching > L2-Redundancy > FuseNet]

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

Note:
If you use the *Ring/Network Coupling* function to couple networks, then verify that the networks only contain Hirschmann devices.

Use the following table to select the *FuseNet* coupling protocol to be used in the network:

Main Ring	Connected Network		
	MRP	HIPER Ring	RSTP
MRP	*Sub Ring*[1)]	*RCP* *Ring/Network Coupling*	*RCP* *Ring/Network Coupling*
HIPER Ring	*Sub Ring*	*Ring/Network Coupling*	*RCP* *Ring/Network Coupling*
RSTP	*RCP*	*RCP*	–

– no suitable coupling protocol

1) with the *MRP* function set up on different VLANs

The menu contains the following dialogs:

- Sub Ring
- Ring/Network Coupling
- Redundant Coupling Protocol

5.9.6.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub Ring]

This dialog lets you set up the device to operate in the *Sub Ring Manager* mode.

The *Sub Ring* function lets you easily couple network segments to existing redundancy rings. The *Sub Ring Manager* device couples a Sub Ring to an existing ring (base ring).

You can integrate any devices that support MRP as participants in the Sub Ring. These devices do not require support for the *Sub Ring* 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 devices participating in the base ring
  - on the base ring ports of the *Sub Ring Manager* device
- VLAN Y for Sub Ring
  - on the ring ports of the devices participating in the Sub Ring
  - on the Sub Ring ports of the *Sub Ring Manager* device

Note:
To help avoid loops, only close the redundant line when the settings are specified in every device participating in the ring.

Operation

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 18.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Sub Ring ID* field, you specify the number that uniquely identifies the Sub Ring.
  Possible values:
  - `1..40000`
    You can replace the value prefilled by the device with any value in the range.

The device lets you set a maximum of 20 Sub Ring instances.

 Remove

Removes the selected table row.

Sub Ring ID

Displays the number that uniquely identifies the Sub Ring.

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 device participating in the Sub Ring 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.

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* device receives data packets from more than one *Sub Ring Manager* devices in the Sub Ring.
- *noPartnerManager*
  The *Sub Ring Manager* device receives its own data packets.
- *concurrentVLAN*
  The Media Redundancy Protocol (MRP) 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 Media Redundancy Protocol (MRP).

Redundancy

Displays if the redundancy is available.

When a component of the Sub Ring becomes inoperable, the redundant line takes over its function.

Possible values:

- *redGuaranteed*
  The redundancy is available.
- *redNotGuaranteed*
  The redundancy is unavailable.

Port

Specifies the port that connects the device to the Sub Ring.

Possible values:

- <Port number>

Administrative mode

Specifies the mode of the *Sub Ring Manager* device.

There are 2 *Sub-Ring Manager* devices that connect the Sub Ring to the base ring. As long as the Sub Ring is physically closed, one *Sub Ring Manager* device 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*.

- *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.

Operational mode

Displays the current mode of the *Sub Ring Manager* device.

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 on 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 interrupted.

Sub Ring status

Displays the operational state of the Sub Ring in the *Sub Ring Manager* domain.

Possible values:

- *undefined*
  Undefined state
- *open*
  The Sub Ring is opened.
- *closed*
  The Sub Ring is closed.

VLAN

Specifies the VLAN to which this Sub Ring is assigned. If no VLAN exists with the specified VLAN ID, then the device sets up the VLAN.

Possible values:

- Available set-up VLANs (default setting: `0`)
  If you do not want to use a separate VLAN for this Sub Ring, then keep the value as `0`.

Partner MAC

Displays the MAC address of the *Sub Ring Manager* device at the other end of the Sub Ring.

MRP domain

Specifies the MRP domain of the *Sub Ring Manager* device. Assign the same MRP domain name to every member of a Sub Ring. If you only use Hirschmann devices, then 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:
  `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protocol

Specifies the protocol.

Possible values:

- *iec-62439-mrp*

5.9.6.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > Ring/Network Coupling]

You use the *Ring/Network Coupling* function to redundantly couple an existing HIPER Ring, MRP Ring, or Fast HIPER Ring to another network or another ring. Verify that the coupling partners are Hirschmann devices.

Note:
With two-switch coupling, verify that you have set up a HIPER Ring, MRP Ring, or Fast HIPER Ring before setting up the *Ring/Network Coupling* function.

In the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog, you can perform the following tasks:
- display an overview of the existing *Ring/Network Coupling*
- set up a *Ring/Network Coupling* instance
- enable/disable the *Ring/Network Coupling* instance
- delete the *Ring/Network Coupling* instance

When configuring the coupling ports, specify the following settings in the *Basic Settings > Port* dialog:

Port type	Bit rate	Port on	Autoneg	Manual configuration
TX	100 Mbit/s	marked	unmarked	*100M FDX*
TX	1 Gbit/s	marked	marked	–
Optical	100 Mbit/s	marked	unmarked	*100M FDX*
Optical	1 Gbit/s	marked	marked	–
Optical	2.5 Gbit/s	marked	–	*2.5G FDX*
Optical	10 Gbit/s	marked	–	*10G*

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

If you set up VLANs, then note the VLAN configuration of the coupling and partner coupling ports. Specify the following settings for the coupling and partner coupling ports:
- *Switching > VLAN > Port* dialog
  - Value in the *Port-VLAN ID* column = 1
  - Checkbox in the *Ingress filtering* column = unmarked
- *Switching > VLAN > Configuration* dialog
  - VLAN membership = T

Independently of the VLAN settings, the device sends the ring coupling frames with VLAN ID 1 and priority 7. Verify that the device sends VLAN 1 frames tagged in the local ring and in the connected network. Tagging the VLAN frames maintains the priority of the ring coupling frames.

The *Ring/Network Coupling* function operates with test packets. The devices send their test packets with a VLAN tag, including VLAN ID 1 and the highest VLAN priority 7. If the unblocked port is a member in VLAN 1 and transmits the data packets without a VLAN tag, then the device also sends test packets.

Operation

Buttons

Reset

Disables the redundancy function and resets the parameters in the dialog to the default setting.

Operation

Enables/disables the *Ring/Network Coupling* function.

Possible values:

- *On*
  The *Ring/Network Coupling* function is enabled.
- *Off* (default setting)
  The *Ring/Network Coupling* function is disabled.

Information

Redundancy

Displays if the redundancy is available.

When a component of the ring becomes inoperable, the redundant line takes over its function.

Possible values:

- *redGuaranteed*
  The redundancy is available.
- *redNotGuaranteed*
  The redundancy is unavailable.

Configuration failure

You have set up the function incorrectly, or there is no ring port connection.

Possible values:

- *noError*
- *slaveCouplingLinkError*
  The coupling line is not connected to the coupling port of the slave device. Instead, the coupling line is connected to another port of the slave device.
- *slaveControlLinkError*
  The control port of the slave device has no data link.
- *masterControlLinkError*
  The control line is not connected to the control port of the master device. Instead, the control line is connected to another port of the master device.
- *twoSlaves*
  The control line connects two slave devices.

- *localPartnerLinkError*
  The partner coupling line is not connected to the partner coupling port of the slave device. Instead, the partner coupling line is connected to another port of the slave device in *one-switch coupling* mode.
- *localInvalidCouplingPort*
  In *one-switch coupling* mode, the coupling line is not connected on the same device as the partner line. Instead, the coupling line is connected to another device.
- *couplingPortNotAvailable*
  The coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.
- *controlPortNotAvailable*
  The control port is not available because the module to which the port refers is not available or the port does not exist on this module.
- *partnerPortNotAvailable*
  The partner coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.

Mode

Type

Specifies the method used to couple the networks together.

Possible values:

- *one-switch coupling* (default setting)
  Lets you specify the port settings in the *Coupling port* and *Partner coupling port* frames.
- *two-switch coupling, master*
  Lets you specify the port settings in the *Coupling port* frame.
- *two-switch coupling with control line, master*
  Lets you specify the port settings in the *Coupling port* and *Control port* frames.
- *two-switch coupling, slave*
  Lets you specify the port settings in the *Coupling port* frame.
- *two-switch coupling with control line, slave*
  Lets you specify the port settings in the *Coupling port* and *Control port* frames.

Coupling port

Port

Specifies the port to which you connect the redundant link.

Possible values:

- *-*
  No port selected.
- *<Port number>*
  If you also have set up ring ports, then specify the coupling and ring ports on different ports.

To help prevent continuous loops, the device disables the coupling port in the following cases:

- disabling the function
- changing the configuration while the connections are operating on the ports

When the device has deactivated the coupling port, the *Port on* checkbox is unmarked in the *Basic Settings > Port* dialog, *Configuration* tab.

State

Displays the status of the selected port.

Possible values:

- `active`
  The port is active.
- `standby`
  The port is in stand-by mode.
- `not-connected`
  The port is not connected.
- `not-applicable`
  The port is incompatible with the set-up control mode.

Partner coupling port

Port

Specifies the port on which you connect the partner port. The field is visible when you select the `one-switch coupling` radio button in the *Mode* frame.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`
  If you also have set up ring ports, then specify the coupling and ring ports on different ports.

Interface index

Displays the index number of the port that the partner device uses for the connection. The field is visible when you select a two-switch coupling method in the *Mode* frame.

State

Displays the status of the selected port.

Possible values:

- `active`
  The port is active.
- `standby`
  The port is in stand-by mode.
- `not-connected`
  The port is not connected.
- `not-applicable`
  The port is incompatible with the set-up control mode.

IP address

Displays the IP address of the partner device, when the devices are connected. The prerequisite is that you enable the partner device in the network. The field is visible when you select a two-switch coupling method in the *Mode* frame.

Control port

Port

Displays the port on which you connect the control line.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

State

Displays the status of the selected port.

Possible values:

- *active*
  The port is active.
- *standby*
  The port is in stand-by mode.
- *not-connected*
  The port is not connected.
- *not-applicable*
  The port is incompatible with the set-up control mode.

Configuration

Redundancy mode

Specifies if the device responds to a detected failure in the remote ring or network.

Possible values:

- *redundant ring/network coupling*
  Either the main line or the redundant line is active. Both lines are not active simultaneously. If the device detects that the link is interrupted between the devices in the remote ring or network, then the standby device keeps the redundant port in the standby mode.
- *extended redundancy* (default setting)
  If the device detects a potential connection interruption between the devices in the remote ring or network, then the standby device forwards data on the redundant port. In this case, the main line and the redundant line are active simultaneously. This setting lets you maintain continuity in the remote network.

Note:
During the reconfiguration period, package duplications can occur. Therefore, if your application is able to detect package duplications, then you can select this setting.

Coupling mode

Specifies the mode of coupling a specific type of network.

Possible values:

- *ring coupling* (default setting)
  The device couples redundant rings. The device lets you couple rings that use the following redundancy protocols:
  - HIPER Ring
  - Fast HIPER Ring
  - MRP Ring
- *network coupling*
  The device couples network segments. The function lets you couple mesh and bus networks together.

5.9.6.3 Redundant Coupling Protocol

[Switching > L2-Redundancy > FuseNet > RCP]

A ring topology provides short transition times with a minimal use of resources. However, to couple these rings redundantly to a higher-level network is more of a challenge.

When you want to use a standard protocol such as MRP for the ring redundancy and RSTP to couple the rings together, the *RCP* function helps provide options for you.

Do not use the following redundancy protocols on the ports of the *RCP* primary ring and the *RCP* secondary rings:

- *Sub Ring*
- *Ring/Network Coupling*

Operation

Operation

Enables/disables the *RCP* function.

Possible values:

- `On`
  The *RCP* function is enabled.
  To help avoid unexpected behavior, do not enable the function on a device on which the *Ring manager* function is enabled.
- `Off` (default setting)
  The *RCP* function is disabled.

Primary ring/network / Secondary ring/network

If the device operates as slave (value in the *Role* field is `slave`), then do not activate the *Static query port* mode for the ports on the secondary ring/network.

Inner port

Specifies the inner port number in the primary ring/secondary ring. The port is directly connected to the partner bridge.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

Outer port

Specifies the outer port number in the primary ring/secondary ring.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

Primary Ring protocol/Secondary Ring protocol

Displays the protocol that is active on the redundant coupling port in the devices in the primary/secondary ring.

If the *RCP* function is disabled, then the device displays the `NONE` value for both primary and secondary ring protocols. If you disable the active protocol on either primary or secondary ring, the device will display the `NONE` value for that respective ring protocol.

Coupler configuration

Role

Specifies the role of the local device.

Possible values:

- `master`
  The device operates as master.
- `slave`
  The device operates as slave.
- `auto` (default setting)
  The device automatically selects its role as *master* or *slave*.

Current role

Displays the current role of the local device. The value can be different from the set-up role:

- If you set up both partner bridges as `auto`, then the partner bridge that is currently coupling the instances takes the `master` role. The other partner bridge takes the `slave` role.
- If both partner bridges are set up as `master` or both as `slave`, then the partner bridge with the smaller Basis MAC address takes the `master` role.
  The other partner bridge takes the `slave` role.
- If the protocol is started and the partner bridge cannot be found for a bridge in the set-up role `master`, `slave` or `auto`, then the bridge sets its own role to `listening`.
- If the device detects a potential configuration problem, for example, the inner ring ports are connected crosswise, then the device sets its role to `error`.

Timeout [ms]

Specifies the maximum time, in milliseconds, during which the slave device waits for test packets from the master device on the outer ports before the slave device takes over the coupling. This only applies in the state in which both inner ports of the slave device have lost the connection to the master device.

Specify the timeout longer than the longest assumable interruption time for the redundancy protocol of the faster instance. Otherwise, loops can occur.

Possible values:

- `5..60000` in steps of 5 (default setting: `250`)
  If you enter a value which is not a multiple of 5, then the device rounds up the value to the nearest multiple of 5.

Partner MAC address

Displays the basic MAC address of the partner device.

Partner primary port

Displays the port of the partner device in the primary ring.

Partner secondary port

Displays the port of the partner device in the secondary ring.

Partner IP address

Displays the IP address of the partner device.

Coupling state

Displays the coupling state of the local device.

Possible values:

- *forwarding*
  The coupling state of the port is forwarding.
- *blocking*
  The coupling state of the port is blocking.

Redundancy state

Displays if the redundancy is available.

For a master-slave configuration, both bridges display this information.

Possible values:

- *redAvailable*
  The redundancy is available.
- *redNotAvailable*
  The redundancy is unavailable.

6 Diagnostics

The menu contains the following dialogs:

- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- LLDP
- Loop Protection
- SFlow
- Report

6.1 Status Configuration

[Diagnostics > Status Configuration]

The menu contains the following dialogs:

- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)

6.1.1 Device Status

[Diagnostics > Status Configuration > 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 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

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 18.

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 the specified upper threshold value or falls below the specified lower threshold value, 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 Ethernet modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove an Ethernet module from the device, then in the *Device status* frame, the value changes to `error`.
  Further below, you have the option of selecting the Ethernet modules to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

Fan module removal

Activates/deactivates the monitoring of the fan modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove a fan module from the device, then in the *Device status* frame, the value changes to `error`.
  Further below, you have the option of selecting the fan modules to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

External memory removed

Activates/deactivates the monitoring of the active external memory (`ENVM`).

Possible values:

- `marked`
  Monitoring is active.
  If you remove the active external memory (`ENVM`) from the device, then in the *Device status* frame, the value changes to `error`.
- `unmarked` (default setting)
  Monitoring is inactive.

You specify the active external memory in the *Basic Settings > Load/Save* dialog, *External memory* frame.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory (`ENVM`).

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 (`ENVM`).
- `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 device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve.
  - The device, as a ring participant, has detected an error in its ring redundancy settings.
- `unmarked` (default setting)
  Monitoring is inactive.

Sub Ring redundancy

Activates/deactivates the monitoring of the Sub Ring redundancy.

Possible values:

- `marked`
  Monitoring is active.
  In the *Device status* frame, the value changes to `error` in the following situations:
  - The device operates as a Sub Ring Manager. The redundancy function of the device uses the alternative Sub Ring connection to the main ring. There is no longer a redundancy reserve within the Sub Ring.
  - The device, as a Sub Ring participant, has detected an error in its Sub Ring redundancy settings.
- `unmarked` (default setting)
  Monitoring is inactive.

Power supply 1
Power supply 2

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 Ethernet 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.

Fan module

Activates/deactivates the monitoring of this fan 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 *Fan module removal* checkbox further up.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 18.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

6.1.2 Security Status

[Diagnostics > Status Configuration > 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

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 18.

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 shorter than 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 1 through the serial interface possible

Activates/deactivates monitoring the option of starting the System Monitor 1.

When active, you can start the System Monitor 1 through the serial connection during system startup.

Possible values:

- `marked`
  Monitoring is active.
  If you activate the option of starting the System Monitor 1, then in the *Security status* frame, the value changes to `error`.
- `unmarked` (default setting)
  Monitoring is inactive.
  If you activate the option of starting the System Monitor 1, the value in the *Security status* frame remains unchanged.

You activate/deactivate the option of starting the System Monitor 1 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 (*ENVM*).

Possible values:

- `marked`
  Monitoring is active.
  If you activate the saving of the configuration profile in the external memory (*ENVM*), 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 (*ENVM*) 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 (*ENVM*).

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the settings allow the device to load an unencrypted configuration profile from the external memory (*ENVM*), 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 (*ENVM*) is unencrypted.
    and
  - The *Config priority* column in the *Basic Settings > External Memory* dialog has the value *first* or *second*.
- `unmarked`
  Monitoring is inactive.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the digital certificate of the HTTPS server.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the HTTPS server uses a self-generated digital certificate, then in the *Security status* frame, the value changes to *error*.
- `unmarked`
  Monitoring is inactive.

Secure Boot is inactive

Activates/deactivates the monitoring of the Secure Boot function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  Until you activate the Secure Boot function, the value in the *Security status* frame continues to display `error`. Once activated, the value changes to `ok`.
- `unmarked`
  Monitoring is inactive.

You activate the Secure Boot function in the *Basic Settings > Software* dialog, *Software update* frame.

Support Mode is active

Activates/deactivates the monitoring of the Support Mode function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the value in the *Security status* frame changes to `error` due to this setting, contact the manufacturer.
- `unmarked`
  Monitoring is inactive.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

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 18.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

6.1.3 Signal Contact

[Diagnostics > Status Configuration > 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

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 18.

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 the specified upper threshold value or falls below the specified lower threshold value, 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.

Ethernet module removal

Activates/deactivates the monitoring of the Ethernet modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove an Ethernet module from the device, then the signal contact opens.
  Further below, you have the option of selecting the Ethernet modules to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

Fan module removal

Activates/deactivates the monitoring of the fan modules.

Possible values:

- `marked`
  Monitoring is active.
  If you remove a fan module from the device, then the signal contact opens.
  Further below, you have the option of selecting the fan modules to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

External memory removed

Activates/deactivates the monitoring of the active external memory (*ENVM*).

You specify the active external memory in the *Basic Settings > Load/Save* dialog, *External memory* frame.

Possible values:

- `marked`
  Monitoring is active.
  If you remove the active external memory (*ENVM*) 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 (*ENVM*).

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 (*ENVM*).
- `unmarked` (default setting)
  Monitoring is inactive.

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 device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve.
  - The device, as a ring participant, has detected an error in its ring redundancy settings.
- `unmarked` (default setting)
  Monitoring is inactive.

Sub Ring redundancy

Activates/deactivates the monitoring of the Sub Ring redundancy.

Possible values:

- `marked`
  Monitoring is active.
  The signal contact opens in the following situations:
  - The device operates as a Sub Ring Manager. The redundancy function of the device uses the alternative Sub Ring connection to the main ring. There is no longer a redundancy reserve within the Sub Ring.
  - The device, as a Sub Ring participant, has detected an error in its Sub Ring redundancy settings.
- `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 1
Power supply 2

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 Ethernet module.

Possible values:

- `marked`
  Monitoring is active.
  If you remove this Ethernet 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.

Fan module

Activates/deactivates the monitoring of this fan module.

Possible values:

- `marked`
  Monitoring is active.
  If you remove this fan module from the device, then the signal contact opens.
- `unmarked` (default setting)
  Monitoring is inactive.

This setting is effective when you mark the *Fan module removal* checkbox further up.

[Port]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 18.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

6.1.4 MAC Notification

[Diagnostics > Status Configuration > 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 (forwarding database). 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

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 (2³¹-1)` (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 18.

Port

Displays the port number.

Active

Activates/deactivates the *MAC Notification* function on the port.

Possible values:

- `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)

[Diagnostics > Status Configuration > Alarms (Traps)]

The device lets you send an SNMP trap in response to specific events.

You specify the events for which the device triggers an SNMP trap in the following dialogs:
- *Diagnostics > Status Configuration > Device Status*
- *Diagnostics > Status Configuration > Security Status*
- *Diagnostics > Status Configuration > MAC Notification*

The menu contains the following dialogs:
- Trap V3 User Management
- Trap Destinations

6.1.5.1 Trap V3 User Management

[Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management]

In this dialog, you specify the SNMPv3 trap users who can send SNMP traps to the trap destination(s). The device supports encrypted SNMPv3 traps and authentication for sending.

SNMPv3 trap users have permission to send SNMPv3 traps to the specified SNMPv3 trap hosts.

SNMPv3 trap users are intended for sending SNMPv3 traps to SNMPv3 trap hosts exclusively. SNMPv3 trap users are different from the user accounts set up in the device. Do not confuse them. See the *Device Security > User Management* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

 Add

Opens the *Create* window to add a table row. The device adds a maximum of 10 SNMPv3 trap users with the parameters you specify in this window.

- From the *User to be cloned* drop-down list, you select the user account, from which the device clones the authentication settings.
  You need to select one of the user accounts set up in the device. You set up device user accounts in the *Device Security > User Management* dialog.
- In the *Trap User name* field, you specify the name for the SNMPv3 trap user.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters
- From the *Trap User Auth Protocol* drop-down list, you select the algorithm that the device uses to authenticate the SNMPv3 traps. The available values depend on the algorithm specified for the user to be cloned.
  Possible values:
  - *none* (default setting)
    No authentication.
  - *hmacmd5*
    MD5
  - *hmacsha*
    SHA-1
  - *hmacsha256*
    SHA-256
- In the *Trap User Auth Password* field, you specify the password that the device uses with the selected algorithm to authenticate the SNMPv3 traps. Required only if from the *Trap User Auth Protocol* drop-down list, an item other than *none* is selected.
  Possible values:
  - Alphanumeric ASCII character string with 8..64 characters

- From the *Trap User Priv Protocol* drop-down list, you select the algorithm that the device uses to encrypt the SNMPv3 traps. The prerequisite is that from the *Trap User Auth Protocol* drop-down list, an item other than *none* is selected. The available values depend on the algorithm specified for the user to be cloned.
  Possible values:
  - *none* (default setting)
    No encryption.
  - *des*
    DES
  - *aesCfb128*
    AES-128
  - *aesCfb256*
    AES-256
- In the *Trap User Priv Password* field, you specify the password that the device uses with the selected algorithm to encrypt SNMPv3 traps. Required only if from the *Trap User Priv Protocol* drop-down list, an item other than *none* is selected.
  Possible values:
  - Alphanumeric ASCII character string with 8..64 characters

When you click the *Ok* button, the device adds the table row for the SNMPv3 trap user. If you have selected an item other than *none* in the *Trap User Auth Protocol* or *Trap User Priv Protocol* drop-down list, the *Credentials* window opens first. Then, you enter the required password(s). Even if you enter an incorrect password, the device still adds the SNMPv3 trap user. However, when the device sends SNMPv3 traps, the trap destination cannot decrypt them.

Remove

Removes the selected table row.

SNMPv3 Notification User

Displays the name of the SNMPv3 trap user.

Authentication

Displays the protocol for sending SNMPv3 traps with authentication in the context of the SNMPv3 trap user.

Auth Password

Specifies the authentication password of the SNMPv3 trap user. The device displays ●●●●● (dots) instead of the password.

To change the password, click the relevant field. The device opens a password entry/change dialog, see “[Password entry/change dialog]” on page 407.

To change the password, add another SNMPv3 trap user and then delete the existing one.

Privacy

Displays the protocol that the device uses for this user to encrypt the SNMPv3 traps.

Priv Password

Specifies the privacy (encryption) password of the SNMPv3 trap user. The device displays ●●●●● (dots) instead of the password.

To change the password, click the relevant field. The device opens a password entry/change dialog, see "[Password entry/change dialog]" on page 407.

To change the password, add another SNMPv3 trap user and then delete the existing one.

User status

Displays the status of the SNMPv3 trap user.

Possible values:

- `marked` (default setting)
  The SNMPv3 trap user is active.
- `unmarked`
  The SNMPv3 trap user is inactive.

[Password entry/change dialog]

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (min.):

This dialog element displays the required minimum length of the password.

- If the currently entered password satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

6.1.5.2 Trap Destinations

[Diagnostics > Status Configuration > Alarms (Traps) > Trap Destinations]

In this dialog, you specify the trap destinations to which the device sends SNMP traps.

For SNMPv3, the following conditions apply:
- The device sends SNMPv3 traps to the trap destination specified for the relevant SNMPv3 trap user.
- The device supports a maximum of 10 trap destinations for SNMPv3.

Operation

Operation

Enables/disables sending SNMP traps.

Possible values:

▶ *On* (default setting)
Sending SNMP traps is enabled.

▶ *Off*
Sending SNMP traps is disabled.

SNMPv1/v2 trap community

Name

Specifies the community string that the device sends in each SNMPv1/v2 trap for authentication to the trap destination.

Possible values:

▶ Alphanumeric ASCII character string with 0..64 characters
`trap` (default setting)

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Add

Opens the *Create* window to add a table row. Thus, you set up a trap destination on the device.

- In the *Name* field, you specify a name for the trap destination.
  Possible values:
  ▶ Alphanumeric ASCII character string with 1..32 characters

- From the *Type* drop-down list, you select the SNMP version which the device uses to send SNMP traps to the trap destination.
  Possible values:
  - `V1`
    SNMP version 1
    Do not use this setting if you transmit data over untrusted networks.
  - `V3`
    SNMP version 3
- In the *Address* field, you specify the IP address and the port of the trap destination.
  Possible values:
  - `<IPv4 address>:<port>`
    If you do not specify a port, then the device automatically adds port `162` to the trap destination.
- From the *SNMPv3 Trap user* drop-down list, you select the SNMPv3 trap user in whose context the device sends SNMPv3 traps to the trap destination.
  The prerequisite is that you select the `V3` item from the *Type* drop-down list.
  You select one of the users that you have set up in the *Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management* dialog.
- From the *Security level* drop-down list, you select whether the device sends the SNMPv3 traps encrypted and whether authentication is required before sending.
  The prerequisite is that you select the `V3` item from the *Type* drop-down list.
  Possible values:
  - *`noAuthNoPriv`*
    The device sends unencrypted SNMPv3 traps without authentication.
    Do not use this setting if you transmit data over untrusted networks.
  - *`authNoPriv`*
    The device sends unencrypted SNMPv3 traps.
    The user needs to authenticate before sending SNMPv3 traps.
  - *`authPriv`*
    The device sends encrypted SNMPv3 traps.
    The user needs to authenticate before sending SNMPv3 traps.


Remove

Removes the selected table row.

Name

Displays the name you specified for the trap destination (trap host).

SNMP Protocol

Displays the SNMP version which the device uses to send SNMP traps to the trap destination.

Address

Specifies the IP address and the port of the trap destination (trap host).

Possible values:

- `<IPv4 address>:<port>`
  If you do not specify a port, then the device automatically adds port `162` to the trap destination.

SNMPv3 Trap user

Specifies the SNMPv3 trap user that the device uses to send SNMPv3 traps to the trap destination.

You select one of the SNMPv3 trap users that you have set up in the *Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management* dialog.

Security level

Specifies whether the device sends the SNMPv3 traps encrypted and whether authentication is required before sending.

Possible values:

- *noAuthNoPriv*
  The device sends unencrypted SNMPv3 traps without authentication.
  Do not use this setting if you transmit data over untrusted networks.
- *authNoPriv*
  The device sends unencrypted SNMPv3 traps.
  The user needs to authenticate before sending SNMPv3 traps.
- *authPriv*
  The device sends encrypted SNMPv3 traps.
  The user needs to authenticate before sending SNMPv3 traps.

Type

Displays the notification type.

Active

Activates/deactivates the sending of SNMP traps to the 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

[Diagnostics > System]

The menu contains the following dialogs:

- System Information
- Hardware State
- Configuration Check
- IP Address Conflict Detection
- ARP
- Selftest

6.2.1 System Information

[Diagnostics > System > 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

Saves the HTML page on your PC using the web browser dialog.

6.2.2 Hardware State

[Diagnostics > System > 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 18.

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

[Diagnostics > System > 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.

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 IEEE 802.1D-2004. 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.

Configuration

Start configuration check...

Starts the check and updates the content of the table.

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.

Information

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 18.



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

[Diagnostics > System > 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

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*
  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*
  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` (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 an address conflict, 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 18.

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

[Diagnostics > System > 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 IPv6, the device obtains the addresses of the neighboring devices 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 18.

Buttons

Clear ARP table

Deletes 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.

Active

Displays that the ARP table contains the IP/MAC address assignment as an active entry.

6.2.6 Selftest

[Diagnostics > System > Selftest]

This dialog lets you do the following:
- Activate/deactivate the RAM self-test the device performs during system startup.
- Activate/deactivate the option of starting the System Monitor 1 during 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 the device performs 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 boot time for the device.

SysMon1 is available

Activates/deactivates the option of starting the System Monitor 1 during system startup.

Possible values:

▶ `marked` (default setting)
During system startup, the boot menu will display the System Monitor 1 item.
To actually start the System Monitor 1, select this item during system startup.

▶ `unmarked`
During system startup, the boot menu will not display the System Monitor 1 item.
No one can start the System Monitor 1.

The System Monitor 1 provides functions for recovering the operating settings of the device.

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. Access to the device management is only possible using the Command Line Interface through the serial connection.
  To regain access to the device through the network, start the System Monitor 1 and reset the settings. After the system startup, the device uses 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 18.

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

[Diagnostics > 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

[Diagnostics > 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

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.

Certificates/CRLs

To establish a secure connection, the device requires to obtain a valid digital certificate to verify the identity of the server. The prerequisite is that you have transferred the public certificate of the server onto the device. Ask the server administrator for a digital certificate in X.509 format. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

A Certificate Revocation List (CRL) contains a list of digital certificates revoked by the Certification Authority (CA) before their scheduled expiration date. When establishing a secure connection to the server, the device stops setting up the connection if the CRL includes the public certificate of the server. The device logs the event in the System Log. For security reasons, Hirschmann recommends using only CRLs signed by a Certification Authority (CA).

Buttons

Clear all Certificates/CRLs

Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (*NVM*).

URL

Specifies the path and file name of the digital certificate or CRL.

The device accepts digital certificates and CRLs with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines
  `-----BEGIN CERTIFICATE-----`
  …
  `-----END CERTIFICATE-----`
  or
  `-----BEGIN CRL-----`
  …
  `-----END CRL-----`

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  When the file 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 through TFTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Transfers the file specified in the *URL* field onto the device.

In this dialog, you can transfer a maximum of 20 digital certificates and additionally a maximum of 20 CRLs onto the device.

For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the *Email Notification* function. See the *Operation* frame.

Sender

Email address

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 urgent

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 non-urgent

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

Severity	Meaning
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical status
error	Error status
warning	Warning
notice	Significant, normal status
informational	Information message
debug	Debug message

6.3.2 Email Notification Recipients

[Diagnostics > 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 18.

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 whether the device sends the emails to this recipient immediately or periodically.

Possible values:

- *urgent* (default setting)
  The device sends the emails to this recipient immediately.
- *non-urgent*
  The device sends the emails to this recipient periodically.

Email 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

[Diagnostics > 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 18.

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.

- From the *Recipient* drop-down list, you select to which recipients the device sends the test email. Possible values:
  - *urgent*
    The device sends the test email to the recipients to which the device sends emails immediately.
  - *non-urgent*
    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`)
- Valid IPv6 address
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
  The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

Destination TCP port

Specifies the TCP port of the server.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `25`)

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. The device displays ●●●●● (dots) instead of the password.

To change the password, click the relevant field. The device opens a password entry/change dialog, see "[Password entry/change dialog]" on page 434.

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.

[Password entry/change dialog]

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

6.4 Syslog

[Diagnostics > 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

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.

Certificates/CRLs

To establish a secure connection, the device requires to obtain a valid digital certificate to verify the identity of the server. The prerequisite is that you have transferred the public certificate of the server onto the device. Ask the server administrator for a digital certificate in X.509 format. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

A Certificate Revocation List (CRL) contains a list of digital certificates revoked by the Certification Authority (CA) before their scheduled expiration date. When establishing a secure connection to the server, the device stops setting up the connection if the CRL includes the public certificate of the server. The device logs the event in the System Log. For security reasons, Hirschmann recommends using only CRLs signed by a Certification Authority (CA).

Buttons

Clear all Certificates/CRLs

Deletes the digital certificates and CRLs transferred onto the device from the non-volatile memory (*NVM*).

URL

Specifies the path and file name of the digital certificate or CRL.

The device accepts digital certificates and CRLs with the following properties:

- X.509 format
- `.PEM` file name extension
- Base64-coded and enclosed by the lines

```
-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----
```

or

```
-----BEGIN CRL-----
…
-----END CRL-----
```

The device gives you the following options for transferring the file onto the device:

- Import from the PC

  When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- Import through FTP
  Do not use this method if you transmit data over untrusted networks.
  When the file 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 through TFTP
  Do not use this method if you transmit data over untrusted networks.
  When the file is on a TFTP server, specify the URL for the file in the following form:
  `tftp://<IP address>/<path>/<file name>`
- Import through SCP or SFTP
  When the file 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>`
    Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.
  - `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

  Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Start

Transfers the file specified in the *URL* field onto the device.

In this dialog, you can transfer a maximum of 32 digital certificates and additionally a maximum of 32 CRLs onto the device.

For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the *Syslog* function. See the *Operation* frame.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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 add a 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
- DNS name in the format `<domain>.<tld>` or `<host>.<domain>.<tld>`
  The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.
  To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

Destination UDP port

Specifies the TCP or UDP port on which the syslog server expects the log entries.

Possible values:

- `1..65535 (2¹⁶-1)` (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.

Possible values:

- `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

[Diagnostics > Ports]

The menu contains the following dialogs:

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring
- RSPAN

6.5.1 SFP

[Diagnostics > Ports > SFP]

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 18.

Port

Displays the port number.

Module type

Type of the SFP transceiver, for example M-SFP-SX/LC.

Serial number

Displays the serial number of the SFP transceiver.

Connector type

Displays the connector type.

Supported

Displays if the device supports the SFP transceiver.

Temperature [°C]

Operating temperature of the SFP transceiver in °Celsius.

Tx power [mW]

Transmission power of the SFP transceiver in mW.

Rx power [mW]

Receiving power of the SFP transceiver in mW.

Tx power [dBm]

Transmission power of the SFP transceiver in dBm.

Rx power [dBm]

Receiving power of the SFP transceiver in dBm.

6.5.2 TP cable diagnosis

[Diagnostics > Ports > 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 a broken cable, it also displays the estimated distance to where it detected the problem.

To receive dependable results, use the *TP cable diagnosis* function for twisted-pair cables with a minimum length of 10 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 successfully performed a test.
- *failure*
  The device detected that the test was interrupted.
- *uninitialized*
  The device has not performed any test yet.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Cable pair

Displays the cable pair to which this table row relates. The device uses the first PHY index supported to display the values.

Result

Displays the results of the cable test.

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*.

Min. length

Displays the minimum estimated length of the cable in meters.

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.

Max. length

Displays the maximum estimated length of the cable in meters.

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.

Distance [m]

Displays the estimated distance in meters from one end of the cable to the other or to an interruption in the cable.

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

[Diagnostics > Ports > 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

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 18.

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:

- `-`
  No monitored parameter.
  The device does not carry out any action.
- *`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 18.

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 18.

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:

- `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 18.

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 (10⁶)` (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 a port if the port operates in any of the following roles:

- Member of a Link Aggregation group

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

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.

Unit

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 *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 (10⁷)` (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 (10⁷)` (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 18.

Port

Displays the port number.

10M 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.

100M 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.

1G 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.

2.5G FDX

Activates/deactivates the port monitor to accept a full-duplex and 2.5 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.

10G

Activates/deactivates the port monitor to accept a full-duplex and 10 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

[Diagnostics > Ports > 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 18.

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 (2³²-1)`
  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.
- `DHCP_SNP`
  DHCP Snooping
  See the *Network Security > DHCP Snooping* dialog.
- `DOT1S`
  BPDU guard
  See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- `DAI`
  Dynamic ARP Inspection
  See the *Network Security > Dynamic ARP Inspection* 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.

- *DHCP snooping*
  Too many DHCP packages from untrusted sources. See the *Network Security > DHCP Snooping > Configuration* dialog, *Port* tab.
- *ARP rate*
  Too many ARP packages from untrusted sources. See the *Network Security > Dynamic ARP Inspection > Configuration* dialog, *Port* 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 18.

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.
- *l2 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

[Diagnostics > Ports > 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 restores the previously applied settings.

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
- Uplink port on which a Layer 2 redundancy protocol is active

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 sends. The destination port sends the unmodified 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 superfluous 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.
  The port sends the same data as the port specified above. Exception:
  - No *VLAN mirroring* data
  - No *RSPAN* data

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.

VLAN mirroring

The *VLAN mirroring* function lets you copy ingress data packets in a specific VLAN to the selected destination port. The device forwards the data stream out of the specified destination port.

Note:
The *VLAN mirroring* function is only available on the primary port.

Source VLAN ID

Specifies the VLAN from which the device mirrors data to the destination port.

Possible values:

- `0` (default setting)
  Disables the *VLAN mirroring* function.
- `2..4042`
  The device lets you specify a VLAN only if no source port is specified.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Source port

Displays the port number.

Active

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.
- `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 sends. The destination port sends the unmodified data packets that the source port receives.

Possible values:

- *none* (default setting)
  No data packets.
- *tx*
  Data packets that the source port sends.

- *rx*
  Data packets that the source port receives.
- *txrx*
  Data packets that the source port sends.

Note:
With the *txrx* setting the device copies each transmitted data packet. 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.

6.5.6 RSPAN

[Diagnostics > Ports > RSPAN]

In this dialog, you specify the settings for the *RSPAN* function. The *RSPAN* function is an extension of the local mirroring function and uses multiple devices in specific roles to forward mirrored data packets to a single *Destination switch*. For that, RSPAN uses an RSPAN VLAN reserved specifically for this purpose.

Using the *RSPAN* function, a *Source switch* mirrors data packets that it receives or sends on the ports or the *Source VLAN* you have selected and sends them on the RSPAN VLAN to a device in another role. An optional *Intermediate switch* transfers the mirrored data packets in the direction of the *Destination switch*. The *Destination switch* makes the data packets accessible on a local port for monitoring and analysis.

Before you set up the *RSPAN* function, decide on the role that the device will operate in:

- *Source switch*
  The device forwards the data packets received or sent on the selected *Source ports* or the *Source VLAN* to the RSPAN VLAN.
- *Destination switch*
  The device receives the data packets from the *Source switches* or *Intermediate switches* on the RSPAN VLAN and makes the packets accessible for monitoring and analysis.
- *Intermediate switch*
  If you use one or more *Intermediate switches* on the path between the *Source switch* and *Destination switch*, then the *Port Mirroring* function is not required for this role.
  You only set up the RSPAN VLAN and make the *Destination port* that is connected to the *Destination switch* or to another *Intermediate switch* a member of this VLAN. See the *Switching* > VLAN > *Configuration* dialog.

Operation

Buttons

Reset config

Resets the settings in the dialog to the default settings.

Operation

Enables/disables the *RSPAN* function.

Possible values:

- *On*
  The *RSPAN* function is enabled.
  The device operates in the *Source switch* or *Destination switch* role, depending on the settings in the *Role* frame.
- *Off* (default setting)
  The *RSPAN* function is disabled.
  The device does not take part in the *RSPAN* function, or it operates in the *Intermediate switch* role, for which no settings are necessary in this dialog.

Role

In the *Role* frame, you specify whether the device operates in the *Source switch* or *Destination switch* role. Depending on your selection, further settings are possible in this dialog either in the [Source switch] tab or the [Destination switch] tab.

Role

Specifies the role that the device will operate in.

Possible values:

- `Source switch` (default setting)
  The device will operate in the *Source switch* role.
- `Destination switch`
  The device will operate in the *Destination switch* role.

[Source switch]

For this role, you specify the *Source ports* or the *Source VLAN*. The device will forward the data packets received or sent on the *Source ports* or on the *Source VLAN* to the *Reflector port* or to the *Destination port*. The device sends the mirrored data packets with the RSPAN VLAN tag.

Reflector port

Reflector port

Specifies the port to which the device internally sends the mirrored data packets. The *Reflector port* then forwards the mirrored data packets to the RSPAN VLAN.

Preparatory steps:

- ☐ Specify an existing VLAN ID in the *RSPAN* frame.
- ☐ Specify the value `-` in the *Destination port* frame.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`

RSPAN

RSPAN Destination VLAN ID

The device tags the mirrored data packets with this VLAN ID and then forwards them to the *Reflector port* or to the *Destination port*. The VLAN 1 is the default VLAN for the device management and cannot be used as the RSPAN VLAN.

Prerequisites:

- In the *Switching > VLAN > Configuration* dialog, the VLAN is already set up.
- In the *Switching > VLAN > Configuration* dialog, the *RSPAN VLAN* column, the checkbox is marked for the particular VLAN.

Possible values:

- `0` (default setting)
  The RSPAN VLAN is inactive as it is not connected to any monitoring session.
- `2..4042`
  Verify that the same VLAN is set up on the *Intermediate switches* and on the *Destination switch*.

Destination port

Destination port

The device forwards the mirrored data packets from the *Source ports* or the *Source VLAN* to this port. The prerequisite is that in the *Reflector port* frame the value `-` is selected.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`
  This port needs sufficient bandwidth to accommodate the data stream. If the mirrored data stream exceeds the bandwidth of this port, then the device discards superfluous data packets on the port.
  The prerequisite is that the port is not used for any of the following purposes:
  - Mirroring source port
  - Layer 2 redundancy protocols

VLAN mirroring

Using VLAN mirroring, the device mirrors data packets that it receives in a specific VLAN to the destination port.

Source VLAN ID

Specifies the VLAN whose data packets the device mirrors to the *Destination port*, if none of the *Source ports* is active.

Prerequisites:

- In the *Switching > VLAN > Configuration* dialog, the VLAN is already set up.
- No source port is active.

Possible values:

- `0` (default setting)
  The *VLAN mirroring* function is disabled.
- `1..4042`

Table

Source port

Displays the port number.

Active

Activates/deactivates the mirroring of data packets that the port receives and sends.

Possible values:

- `marked`
  The device mirrors the data packets that the port receives and sends.
  The device can mirror up to 8 ports simultaneously.
- `unmarked` (default setting)
  The device does not mirror the data packets that the port receives and sends.
  Use this setting for the *Reflector port* and the *Destination port*.

Type

Specifies which data packets the device mirrors on this port.

Possible values:

- *`none`* (default setting)
  The device does not mirror the data packets that the port receives and sends.
- *`tx`*
  The device mirrors the data packets that the port sends.
- *`rx`*
  The device mirrors the data packets that the port receives.
- *`txrx`*
  The device mirrors the data packets that the port receives and sends.

[Destination switch]

In the *Destination switch* role, the device serves as the destination for mirrored data packets originating from other devices.

RSPAN

RSPAN Source VLAN ID

The device forwards each data packet received in this VLAN to the specified *Destination port*. The VLAN 1 is used to access the device management and cannot be used as the RSPAN VLAN.

Prerequisites:

- In the *Switching > VLAN > Configuration* dialog, the VLAN is already set up.
- In the *Switching > VLAN > Configuration* dialog, the *RSPAN VLAN* column, the checkbox is marked for the particular VLAN.

Possible values:

- `0` (default setting)
  The RSPAN VLAN is inactive as it is not connected to any monitoring session.
- `2..4042`
  Verify that the same VLAN is set up on the *Intermediate switches* and on the *Destination switch*.

Destination port

Destination port

The device forwards the RSPAN data packets that it receives from the *Source switches* or *Intermediate switches* to this port.

Possible values:

- `-` (default setting)
  No port selected.
- `<Port number>`
  This port needs sufficient bandwidth to accommodate the data stream. If the mirrored data stream exceeds the bandwidth of this port, then the device discards superfluous data packets on the port.
  The prerequisite is that the port is not used for any of the following purposes:
  - Mirroring source port
  - Layer 2 redundancy protocols

6.6 LLDP

[Diagnostics > 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 the network.

This menu lets you set up the topology discovery and to display the information received in tabular form.

The menu contains the following dialogs:

- LLDP Configuration
- LLDP Topology Discovery

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

This dialog lets you set up the topology discovery for every port.

Operation

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 sends LLDP data packets.

Possible values:

- `5..32768 (2¹⁵)` (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 the device settings change.

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 18.

Port

Displays the port number.

Operation

Specifies if the port transmits LLDP data packets.

Possible values:

- *transmit*
  The port sends LLDP data packets but does not save any information about neighboring devices.
- *receive*
  The port receives LLDP data packets but does not send 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 send LLDP data packets and does not save information about neighboring devices.

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 sends the TLV with the port description.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the device name.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the system description.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 sends the TLV with the system capabilities.
- `unmarked`
  The transmitting of the TLV is inactive.
  The device does not send 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 MAC address table (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

[Diagnostics > 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 the 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 MAC address table (forwarding database) 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 18.

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 MAC address table (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 auto-negotiation.

Autonegotiation

Displays if auto-negotiation 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 18.

Port

Displays the port number.

Device class

Displays the device class of the remotely connected device.

Possible values:

- *notDefined*
  The device has capabilities not covered by any of the *LLDP-MED* classes.
- *endpointClass1*
  The device has *endpointClass1* capabilities.
- *endpointClass2*
  The device has *endpointClass2* capabilities.
- *endpointClass3*
  The device has *endpointClass3* capabilities.
- *networkConnectivity*
  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.

- 0
  Priority tagged packets
  Only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port.
- 1..4042
  Valid Port VLAN ID

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.

Possible values:

- *true*
  The network policy for the specified application type is currently unknown. In this case, the device ignores the Layer 2 priority and value of the *DSCP* field.
- *false*
  Indicates a specified network policy.

Tagged bit status

Displays the tagged bit status.

Possible values:

- *true*
  The application uses a tagged VLAN.
- *false*
  For the specific application the device uses untagged VLAN operation. In this case, the device ignores both the VLAN ID and the Layer 2 priority fields. The DSCP value on Layer 3, however, is relevant.

Hardware revision

Displays the vendor-specific hardware revision string as advertised by the remote endpoint.

Firmware revision

Displays the vendor-specific firmware revision string as advertised by the remote endpoint.

Software revision

Displays the vendor-specific software revision string as advertised by the remote endpoint.

Serial number

Displays the vendor-specific serial number as advertised by the remote endpoint.

Manufacturer name

Displays the vendor-specific manufacturer name as advertised by the remote endpoint.

Model name

Displays the vendor-specific model name as advertised by the remote endpoint.

Asset ID

Displays the vendor-specific asset tracking identifier as advertised by the remote endpoint.

6.7 Loop Protection

[Diagnostics > 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

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

Auto-disable

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` (default setting: `5`)

Receive threshold

Specifies the threshold value for the number of consecutive *loop detection* packets received. If the number reaches or exceeds this threshold value, then the device will perform the action specified in the *Action* column.

Possible values:

- `1..50` (default setting: `1`)

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Clear port statistics

Resets the values in the following columns:

- *Loops*
- *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.

Loops

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 SFlow

[Diagnostics > SFlow]

sFlow is a standard protocol for monitoring networks. The device contains the sFlow feature which gives you visibility into network activity, allowing for effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent and a central sFlow collector. The agent uses the following forms of sampling:
- statistical packet-based sampling of packet flows
- time-based sampling of counters

The device combines both types of samples into datagrams. sFlow uses the datagrams to forward the sampled data packet statistics to an sFlow collector for analysis.

To perform packet flow sampling, you set up an instance with a sampling rate. You then set up the instance with a polling interval for counter sampling.

The menu contains the following dialogs:
- SFlow Configuration
- SFlow Receiver

6.8.1 SFlow Configuration

[Diagnostics > SFlow > Configuration]

This dialog displays device parameters and lets you set up sFlow instances.

The dialog contains the following tabs:
- [Global]
- [Sampler]
- [Poller]

[Global]

Information

Version

Displays the MIB version, the organization responsible for agent implementation, and the device software revision.

IP address

Displays the IP address associated with the agent providing SNMP connectivity.

[Sampler]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the physical source of data for the sampler.

Receiver

Specifies the receiver index associated with the sampler.

Possible values:
- `-` (default setting)
- `(1)..(8)`
  The value refers to the corresponding *Index* settings specified in the *Diagnostics > SFlow >* Receiver dialog.

Sampling rate

Specifies the static sampling rate for the sampling of the packets from this source.

Possible values:

- `0` (default setting)
  Deactivates the sampling.
- `256..65536`

  When you click the ✓ button after changing the value, the device changes the value to the closest value that the device hardware supports. When the ports receive data, the device increments to the set value and then samples the data.

Max. header size [byte]

Specifies the maximum header size in bytes copied from a sampled packet.

Possible values:

- `20..256` (default setting: `128`)

[Poller]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the physical source of data for the poller counter.

Receiver

Specifies the receiver index associated with the query counter.

Possible values:

- `-` (default setting)
- `(1)..(8)`
  The value refers to the corresponding *Index* settings specified in the *Diagnostics > SFlow > Receiver* dialog.

Interval [s]

Specifies the maximum number of seconds between successive samples of the counters which are associated with this data source.

Possible values:

- `0..86400` (default setting: `0`)

A sampling interval with the value `0` deactivates the sampling of the counters.

6.8.2 SFlow Receiver

[Diagnostics > SFlow > Receiver]

To help avoid a condition where 2 persons or organizations attempt to assume control of the same sampler, the person or organization sets both the *Name* and *Timeout [s]* parameters in the same *SNMP Set request*.

When releasing a sampler, the controlling person or organization deletes the value in the *Name* column or sets the value in the *Timeout [s]* field to `0`. The device then resets the other parameters in this row to their default values.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Index

Displays the index number to which the table row relates.

Name

Specifies the name of the person or company which controls the receiver. Edit this field before making changes to other sampler parameters.

Possible values:

- Alphanumeric ASCII character string with 0..127 characters
  An empty field indicates that the settings in this table row are currently unused.

Timeout [s]

Specifies the time, in seconds, remaining before the sampler is released and stops sampling.

Possible values:

- `-1`
  No timeout. The device does not release the sampler and does not stop sampling.
- `0` (default setting)
  The timeout has expired. The sampler is released and the sampling has stopped. The device resets the other parameters in this row to their default values.
- `1..2147483647 (2³¹-1)`

Datagram size [byte]

Specifies the maximum number of data bytes that are sent in one sample datagram.

Possible values:

- `200..3996` (default setting: `1400`)

IP address

Specifies the IP address of the sFlow collector.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Destination UDP port

Specifies the number of the UDP port for sFlow datagrams.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `6343`)

Datagram version

Displays the version of sFlow datagrams requested.

6.9 Report

[Diagnostics > Report]

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

6.9.1 Report Global

[Diagnostics > 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 487.

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 487.

The device outputs the messages on the serial interface.

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*

- *informational*
- *debug*

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 generates 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 adding 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 for the reception of *SNMP Get requests*.

Possible values:

- *On*
  The logging is enabled.
  The device logs each received *SNMP Get request* as an event 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 for the reception of *SNMP Set requests*.

Possible values:

- *On*
  The logging is enabled.
  The device logs each received *SNMP Set request* as an event 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 logs for received *SNMP Get requests*. For further information, see “Meaning of the event severities” on page 487.

Possible values:

- *emergency*
- *alert*
- *critical*

- *error*
- *warning*
- *notice* (default setting)
- *informational*
- *debug*

Severity set request

Specifies the severity of the event that the device logs for received *SNMP Set requests*. For further information, see “Meaning of the event severities” on page 487.

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 487.

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

File name	Format	Comments
`audittrail.html`	HTML	Contains the chronological recording of the system events and saved user changes in the *Audit Trail* protocol.
`config.xml`	XML	Contains the settings of the device saved in the "Selected" configuration profile. The file name is the same as the name of the current "Selected" configuration profile.
`defaultconfig.xml`	XML	Contains the default settings of the device.
`runningconfig.xml`	XML	Contains the current operating settings of the device.
`script`	TEXT	Contains the output of the command `show running-config script`.
`supportinfo.html`	HTML	Contains device internal service information.
`systeminfo.html`	HTML	Contains information about the current settings and operating parameters.
`systemlog.html`	HTML	Contains the logged events in the Log file. See the *Diagnostics* > Report > *System Log* dialog.

Meaning of the event severities

Severity	Meaning
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical status
error	Error status
warning	Warning
notice	Significant, normal status
informational	Information message
debug	Debug message

6.9.2 Persistent Logging

[Diagnostics > Report > Persistent Logging]

The device lets you save log entries permanently in a file in the external memory (*ENVM*). 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 generated file.

In the table the device displays you the log files held in the external memory (*ENVM*). 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 (*ENVM*).

Note:
Verify that an external memory (*ENVM*) is connected. To verify if an external memory (*ENVM*) 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 removed* parameter in the *Diagnostics > Status Configuration > Device Status* dialog.

Operation

Operation

Enables/disables the *Persistent Logging* function.

Only activate this function if the external memory (*ENVM*) 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 (*ENVM*).
- *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 generated 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 (*ENVM*).

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 (*ENVM*).

Possible values:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (default setting)
- *notice*
- *informational*
- *debug*

Log file target

Specifies the external memory device for logging.

Possible values:

- *sd* (default setting)
  External SD memory (ACA31)
- *usb*
  External USB memory (ACA22)

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons

Clear persistent log file

Deletes the log files from the external memory (*ENVM*).

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 (*ENVM*).

Possible values:

- `messages`
- `messages.X`

File size [byte]

Displays the size of the log file in the external memory (*ENVM*) in bytes.

6.9.3 System Log

[Diagnostics > Report > System Log]

This dialog displays the System Log file. The device logs device-internal events in the System Log file. The device keeps the logged events even after a restart.

To search the System Log file, use the search function of your web browser.

The dialog lets you download a copy of the System Log file onto your computer. The device provides the file to be downloaded in HTML format.

Buttons

 Save log file

Downloads a copy of the System Log file onto your computer, based on the web browser settings.

 Clear log file

Clears the System Log file on the device.

6.9.4 Audit Trail

[Diagnostics > Report > Audit Trail]

This dialog displays the Audit Trail. The dialog lets you save the log file as an HTML file on your PC.

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 to 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 into the device management 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 consecutive 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 device software updates
- Configuration changes using HiDiscovery
- Device software updates and automatic configuration of the device through the external memory (*ENVM*)
- 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 system startup, access to the System Monitor 1 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 1. 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 1. See the *Diagnostics > System > Selftest* dialog, *SysMon1 is available* checkbox.

Buttons



Save audit trail file

Saves the HTML page on your PC using the web browser dialog.

7 Advanced

The menu contains the following dialogs:
- DHCP
- DNS
- Tracking
- Command Line Interface

7.1 DHCP

[Advanced > DHCP]

The menu contains the following dialogs:
- DHCP Server
- DHCP L2 Relay

7.1.1 DHCP Server

[Advanced > DHCP > DHCP Server]

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The menu contains the following dialogs:
- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

7.1.1.1 DHCP Server Global

[Advanced > DHCP > DHCP Server > Global]

This dialog lets you activate the *DHCP Server* function either globally or per port according to your requirements.

Operation

Operation

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

Possible values:

- `On`
- `Off` (default setting)

Configuration

IP probe

Activates/deactivates the probing for unique IP addresses. Before assigning an IP address, the device sends an *ICMP echo request* packet 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 18.

Port

Displays the number of the physical port on which the device listens for DHCP requests and reponds to the client devices.

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.

7.1.1.2 DHCP Server Pool

[Advanced > DHCP > DHCP Server > Pool]

In this dialog, you specify the settings for assigning a certain IP address to client devices from which the device receives a DHCP request.

The device assigns an IP address from a specific pool (address range) depending on which physical port the requesting client device is connected to or in which VLAN it is a member. The MAC address of the requesting client device is a further criterion for the pool from which the device assigns an IP address.

If specified, the device processes further information to assign an IP address from a certain pool to the client device. This can be, for example, the following information in the DHCP request:
- *Circuit ID*
- *Class ID*
- *Client ID*
- *Remote ID*

The device provides a maximum of 128 pools. Up to 1000 client devices can receive their IP settings from the device.

The device manages the IP settings in two types of pools.
- Static pools
  To assign the same IP address to a specific device each time, the device manages the relevant IP settings in a pool whose address range is exactly one IP address.
  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.
- Dynamic pools
  To assign IP addresses from a certain address range, the device manages the relevant IP settings in a pool whose address range includes multiple IP addresses.
  Dynamic pools are useful, for example, to assign a certain IP address to client devices that belong to a certain VLAN.

In addition to the IP settings, the device can assign further parameters (DHCP options) to the client devices. Assigning such parameters is an smart way to automatically set up client devices as they obtain their IP settings. The device lets you specify such parameters for each pool.

The device lets you specify the boot parameters for PXE-compliant clients to boot a bootloader image downloaded from a TFTP server. Possible applications include booting an installation environment, a rescue system, or a live system over the network.

To activate the PXE boot extension for a specific pool, you add the following values to the pool settings:
- *Vendor Identifier*
- *Client System Architecture*
- URL to a bootloader image file on a TFTP server

The device expects the information for *Vendor Identifier* and *Client System Architecture* in summarized form as the *Class Identifier* in the DHCP option 60 field. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool.

Note:
The device does not check the integrity, authenticity and availability of the TFTP servers and the bootloader image files involved. Use the PXE boot extension only if you trust the transfer network. Otherwise, undesirable behavior and security risks may result.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

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.

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 range start

Specifies the fixed IP address for a static pool or the start IP address of an address range.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

IP range end

Specifies the end IP address of an address range. For a static pool, keep the default setting or add the same value as specified in the *IP range start* column.

Possible values:

- Valid IPv4 address (default setting: `0.0.0.0`)

Port

Specifies the number of the physical port on which the requesting client device is connected.

Possible values:

- `All` (default setting)
  The device assigns an IP address to the requesting client device regardless of the port on which the local device receives the DHCP request.
- `<Port number>`
  The device assigns an IP address to the requesting client device only if the local device receives the DHCP request on the specified port.
  The prerequisite is that the item `-` is selected from the drop-down list in the *VLAN ID* column.

VLAN ID

Specifies the VLAN to which the table row relates. The prerequisite is that the item `All` is selected from the drop-down list in the *Port* column.

Possible values:

- `-` (default setting)
- `1..4042`
  The value `1` represents the VLAN in which device management is accessible in the default setting.

MAC address

Specifies the MAC address of the requesting client device.

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 device receives a DHCP request through a different DHCP relay, it ignores this DHCP 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 DCHP 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 DCHP 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`

Vendor ID

Specifies the *Vendor Identifier*. If specified, the device activates the PXE boot extension for the relevant pool. Only use this setting if you transmit the bootloader image file over trusted networks.

When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool.

A matching *Class Identifier* contains the following information:

- The string specified here.
- The value selected in the *Client Architecture* column.

Possible values:

- `-` (default setting)
  The PXE boot extension is inactive for the relevant pool.
  The device ignores the *Class Identifier* in the DHCP option 60 field of received *DHCP Discover* messages.
- Alphanumeric ASCII character string with 1..9 characters

Client Architecture

Specifies the *Client System Architecture*. If specified, the device activates the PXE boot extension for the relevant pool. Only use this setting if you transmit the bootloader image file over trusted networks.

When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool.

A matching *Class Identifier* contains the following information:

- The string specified in the *Vendor ID* column.
- The value selected here.

Possible values:

- `intel-x86pc` (default setting)
  Intel x86 architecture, the common architecture for most desktop PCs and servers
- `nec-pc98`
  NEC's PC-98 series, a PC series based on the x86 architecture
- `efi-itanium`
  Intel Itanium 64-bit processor architecture with EFI (Extensible Firmware Interface)
- `dec-alpha`
  DEC Alpha processor architecture
- `arc-x86`
  Advanced RISC Computing, a variant of the x86 architecture used in specific systems
- `intel-lean-client`
  Intel architecture designed for thin clients
- `efi-ia32`
  Intel Architecture 32-bit with EFI, typically used on older Intel processors (32-bit version of x86)
- `efi-bc`
  Boot Continuity platform using EFI
- `efi-xscale`
  Intel Xscale, a microprocessor series based on ARM architecture, used in embedded systems
- `efi-x86-64`
  x86-64 architecture, also known as AMD64 or Intel 64, with EFI

Hirschmann device

Activates/deactivates the Hirschmann multicasts. If the device in this IP address range serves only Hirschmann client devices, then activate this function.

Possible values:

- `marked`
  In this IP address range, the device serves only Hirschmann client devices. The Hirschmann multicasts are activated.
- `unmarked` (default setting)
  In this IP address range, the device serves client devices of different manufacturers. The Hirschmann multicasts are deactivated.

Configuration URL

Specifies the URL to a file containing additional settings for the client device to get up and running.

If you have specified a value in the *Vendor ID* column and selected a value in the *Client Architecture* column, the URL refers to a bootloader image file on a TFTP server. A PXE-compliant client boots using the file provided in the URL.

Possible values:

- Alphanumeric ASCII character string with 0..70 characters
  When you leave this field blank, the device leaves this option field blank in the *DHCP Offer* message.
  Example: `tftp://192.168.1.10/path/file.name`

Lease time [s]

Specifies the limited period in seconds for which the device leases each IP address.

The client device is responsible for renewing the IP address before the period expires. If the client device does not renew its IP address in time, then the IP address returns to the address pool.

Possible values:

- `60..220752000 (2555 d)` (default setting: `86400`)
- `4294967295 (2³²-1)`
  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`)

NTP server

Specifies the IP address of an external NTP 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`)

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

7.1.1.3 DHCP Server Lease Table

[Advanced > DHCP > DHCP Server > Lease Table]

This dialog displays the currently assigned IP addresses for each port.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the number of the port through which the device to which the IP address is assigned is connected.

IP address

Displays the IP address to which the table row relates.

Status

Displays the lease phase.

According to the standard for DHCP operations, there are 4 phases when assigning 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*
  The 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 how long the assigned IP address is still valid.

Leased MAC address

Displays the MAC address of the device to which the IP address is assigned.

Gateway

Displays the Gateway IP address of the device to which the IP address is assigned.

Client ID

Displays the *client ID* of the device to which the IP address is assigned.

Remote ID

Displays the *remote ID* of the device to which the IP address is assigned.

Circuit ID

Displays the *circuit ID* of the device to which the IP address is assigned.

7.2 DHCP L2 Relay

[Advanced > 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

7.2.1 DHCP L2 Relay Configuration

[Advanced > 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

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 18.

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.

[VLAN ID]

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

VLAN ID

VLAN to which the table row relates.

Active

Activates/deactivates the *DHCP L2 Relay* function in this 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.

7.2.2 DHCP L2 Relay Statistics

[Advanced > 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 18.

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.

7.3 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 hostnames into IP addresses. This name resolution lets you contact other devices using their hostnames 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

[Advanced > DNS > Client > Global]

In this dialog, you enable the *Client* function and the *Cache* function.

Operation

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

Buttons

Flush cache

Deletes every entry from the DNS cache.

Cache

Enables/disables the *Cache* function.

Possible values:

- *On* (default setting)
  The *Cache* function is enabled.
  The device caches up to 128 DNS server responses (hostname and corresponding IP address). When the cache contains a matching entry, the hostname 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

[Advanced > 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 18.

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

[Advanced > DNS > Client > Static]

In this dialog, you specify the DNS servers to which the device forwards requests for resolving hostnames 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

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 RFC 1034 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 18.

Buttons



Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
  Possible values:
  ▶ `1..4`
  The device lets you specify up to 4 external DNS servers.
- In the *IP address* field, you specify the IP address of the DNS server.
  Possible values:
  – Valid IPv4 address
  – Valid IPv6 address



Remove

Removes the selected table row.

Index

Displays the sequential number of the DNS server. You specify the index number when you add a table row.

IP address

Specifies the IP address of the DNS server.

Possible values:

▶ Valid IPv4 address
▶ Valid IPv6 address

Active

Activates/deactivates the table row.

Prerequisites:

- In the *Advanced > DNS > Client > Global* dialog the *DNS client* function is enabled.
- In the *Configuration* frame, the item `user` is selected from the *Source* drop-down list.

Possible values:

- `marked` (default setting)
  The table row is active.
  The device sends requests to the DNS server specified in the first active table row. When the device does not receive a response from this server, it sends the requests to the DNS server specified in the next active table row. The relevant timeout is specified in the *Configuration* frame, *Request timeout [s]* field.
- `unmarked`
  The table row is inactive.
  The device does not send requests to this DNS server.

7.3.1.4 DNS Client Static Hosts

[Advanced > 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 18.

Buttons

 Add

Opens the *Create* window to add a table row.

- In the *Index* field, you specify the index number.
  Possible values:
  ▶ `1..64`
  The device lets you specify up to 64 static hosts.
- In the *Hostname* field, you specify the hostname of the related device.
  Possible values:
  – Alphanumeric ASCII character string with 1..255 characters
- In the *IP address* field, you specify the IP address of the related device.
  Possible values:
  – Valid IPv4 address
  – Valid IPv6 address

 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.

Hostname

Specifies the hostname.

Possible values:

- Alphanumeric ASCII character string with 1..255 characters

IP address

Specifies the IP address under which the host is reachable.

Possible values:

- Valid IPv4 address
- Valid IPv6 address

Active

Activates/deactivates the table row.

Possible values:

- `marked` (default setting)
  The table row is active.
  When the device receives a request for this hostname, it provides the requesting client device with the associated IP address.
- `unmarked`
  The table row is inactive.
  When the device receives a DNS request for this hostname, it forwards the request to a DNS server specified in the *Advanced > DNS > Client > Static* dialog.

7.3.2 OPC UA Server

[Advanced > Industrial Protocols > 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

Listening port

Specifies the TCP port number that the *OPC UA Server* server uses for communication.

Possible values:

- `1..65535 (2¹⁶-1)` (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 18.

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. The device displays ●●●●● (dots) instead of the password.

To change the password, click the relevant field. The device opens a password entry/change dialog, see “[Password entry/change dialog]” on page 519.

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.

[Password entry/change dialog]

If you click a Password field, the device displays a password change dialog. The dialog lets you specify a valid password by displaying the required password criteria. The dialog gives you feedback on which criteria the currently entered password meets.

- The dialog checks if the entered password matches the required password length.
- The dialog checks if the entered password contains only allowed characters.
- The dialog helps avoid typos in the password by having you enter the password twice.

Password length (min.):

This dialog element displays the required minimum length of the password.

- If the currently entered password satisfies the required minimum length:
  - The device displays a green checkmark to the left of the text *Password length (min.):*
  - The device displays the text *Password length (min.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Password length (max.):

This dialog element displays the required maximum length of the password.

- If the password satisfies the required maximum length:
  - The device displays a green checkmark to the left of the text *Password length (max.):*
  - The device displays the text *Password length (max.):* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Contains only allowed characters

This dialog element shows if the password contains only allowed characters:

- If yes:
  - The device displays a green checkmark to the left of the text *Contains only allowed characters*.
  - The device displays the text *Contains only allowed characters* in green.
- If not:
  - The device displays a red exclamation mark (!) to the left of the text.
  - The device displays the text in red.

Enter new password

Enter the new or changed password here. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Confirm password* field.

Confirm password

Confirms the new or changed password. The device displays ●●●●● (dots) instead of the password.

The password entered in this field has to match the value in the *Enter new password* field.

OK

Clicking this button closes the dialog and applies the password to the Password field in the underlying dialog, provided:

- The currently entered password matches every required criteria.
- The *Confirm password* value matches the *Enter new password* value.

Cancel

Clicking this button aborts the dialog and leaves the password in the underlying dialog unchanged.

7.3.3 Service Discovery

[Advanced > Industrial Protocols > Service Discovery]

Service Discovery is part of a series of technologies summarized by the term Zero-configuration networking (zeroconf). Service Discovery uses multicast DNS (mDNS) and DNS service discovery (DNS-SD) to advertise the services offered by the device to other devices in the network that request the service. The device currently supports the *ITxPT Module Inventory* service. Additional services may follow in future releases.

Devices that support Service Discovery can automatically discover the available services on the network without having information about which devices are available. In public transportation, for example, such devices can be ticketing systems, passenger information systems, or vehicle tracking systems.

Devices that subscribe to the services will detect a new device as soon as you connect it to the network, and read its service data. For example, when you install a ticketing system in the network of a public transportation vehicle, the ticketing system needs to communicate with the existing passenger information system to deliver real-time updates on ticket sales and availability.

In this dialog, you select and set up the services that the device will advertise.

The dialog contains the following tabs:
- [ITxPT Module Inventory]

[ITxPT Module Inventory]

The *ITxPT Module Inventory* service is part of the Information Technology for Public Transport (ITxPT) specification.

The intended use of the *ITxPT Module Inventory* service is module inventory in networks of vehicles. The *ITxPT Module Inventory* service lets devices subscribing to the service automatically inventory the modules installed in the on-board IP network of vehicles. Modules in the sense of ITxPT might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. The service lets you collect information about the modules and monitor their status.

The device provides the information through *SRV records* and *TXT records*.
- The *SRV record* contains the location.
- The device provides the *TXT record* through mDNS.
  The *TXT record* contains information about the service.

The device transmits the *TXT record* once in the following cases:
- After an mDNS query containing the address `_itxpt_socket._tcp.local`.
  The device transmits the *TXT record* in response to multicast or unicast requests in the network for services offered by the device.
- Without a request
  - As soon as the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled. See the *Operation* frame.
  - If the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled, and the device detects changes regarding the global status or the port status of other devices in the network. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

Operation

Operation

Enables/disables the *Service Discovery* function. Simultaneously, the device activates/deactivates the *ITxPT Module Inventory* service to monitor the link status of the device.

Possible values:

- *On*
  The *Service Discovery* function is enabled.
  The *ITxPT Module Inventory* service is active.
  The device performs the following actions:
  - On ports for which the checkbox in the *Link* column is marked:
    Monitoring the link status.
    Writing the link status into the *xstatus* attribute of the *TXT record*.
  - The device sends the *TXT record* one time to the devices subscribing to this service.

  The device sends the *TXT record* without a request in the following cases:
  - When you enable the *Service Discovery* function.
    or
  - When the device detects a change regarding the global status or the port status of other devices in the network. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.
- *Off* (default setting)
  The *Service Discovery* function and the *ITxPT Module Inventory* service are disabled.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Port

Displays the port number.

Link

Activates/deactivates the *ITxPT Module Inventory* service to monitor the link status of this port.

Possible values:

- `marked` (default setting)
  The device performs the following actions:
  - Monitoring the link status of this port.
  - Writing the link status into the *xstatus* attribute of the *TXT record*.
  - Transmitting the *TXT record* once, without a request being required.

  Other devices subscribing to this service data can analyze the data contained in the *TXT record*. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.
- `unmarked`
  The device does not monitor the link status of this port.

7.4 Tracking

[Advanced > Tracking]

The tracking function lets you monitor what are known as tracking objects. Examples of monitored tracking objects are the link status of an interface or the reachability of a remote router or end device.

The device forwards status changes of the tracking objects to the registered applications, for example to the routing table or to a VRRP instance. The applications then react to the status changes:

- In the routing table, the device activates/deactivates the route linked to the tracking object.
- The VRRP instance linked to the tracking object reduces the priority of the virtual router so that a backup router takes over the role of the master.
- When the status of the tracking object changes, the device enables/disables the interface linked to the tracking object. The device displays the corresponding application in the *Advanced* > Tracking > *Applications* dialog.

If you set up the tracking objects in the *Advanced* > *Tracking* > *Configuration* dialog, then you can link applications with the tracking objects:

- You link static routes with a tracking object in the *Routing* > *Routing Table* dialog, *Track name* column.
- You link virtual routers with a tracking object in the *Routing* > *L3-Redundancy* > *VRRP* > *Tracking* dialog. Click the button to open the *Create* window and select the tracking object from the *Track name* drop-down list.
- You link the interface status with a tracking object in the *Basic Settings* > *Port* dialog, *Track name* column.

The menu contains the following dialogs:

- Tracking Configuration
- Tracking Applications

7.4.1 Tracking Configuration

[Advanced > Tracking > Configuration]

In this dialog, you set up the tracking objects.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Buttons


Add

Opens the *Create* window to add a table row.

- From the *Type* drop-down list, you select the type of the tracking object.
  Possible values:
  - *interface*
    The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
  - *logical*
    The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.
- In the *Track ID* field, you specify the identification number of the tracking object.
  Possible values:
  - 1..256


Remove

Removes the selected table row.

Type

Specifies the type of the tracking object.

Possible values:

- *interface*
  The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
- *logical*
  The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

Track ID

Specifies the identification number of the tracking object.

Possible values:

- 1..256
  This range is available to every type (*interface*, *ping* and *logical*).

Track name

Displays the name of the tracking object made up of the values displayed in the *Type* and *Track ID* columns.

Active

Activates/deactivates the monitoring of the tracking object.

Possible values:

- `marked`
  Monitoring is active. The device monitors the tracking object.
- `unmarked` (default setting)
  Monitoring is inactive.

Description

Specifies the description.

Here you describe what the device uses the tracking object for.

Possible values:

- Alphanumeric ASCII character string with 0..255 characters

Status

Displays the monitoring result of the tracking object.

Possible values:

- *up*
  The monitoring result is positive:
  - The link status is active.
    or
  - The remote router or end device is reachable.
    or
  - The result of the logical link is *TRUE*.
- *down*
  The monitoring result is negative:
  - The link status is inactive.
    or
  - The remote router or end device is not reachable.
    or
  - The result of the logical link is *FALSE*.
- *notReady*
  The monitoring of the tracking object is inactive. You activate the monitoring in the *Active* column.

Changes

Displays the number of status changes since the tracking object has been activated.

Last changed

Displays the time of the last status change.

Send trap

Activates/deactivates the sending of an SNMP trap when someone activates or deactivates the tracking object.

Possible values:

- `marked`
  If someone activates or deactivates the tracking object in the *Active* column, then the device sends an SNMP trap.
- `unmarked` (default setting)
  The device does not send an SNMP trap.

Port

Specifies the interface to be monitored for tracking objects of the *interface* type.

Possible values:

- `<Interface number>`
  Number of the physical ports or of the link aggregation, LRE or VLAN router interface.
- `no Port`
  No tracking object of the *interface* type.

Link up delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as positive. If the link has been active on the interface for longer than the period specified here, then the *Status* column displays the value *up*.

Possible values:

- `0..255`
- `-`
  No tracking object of the *logical* type.

Link down delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as negative. If the link has been inactive on the interface for longer than the period specified here, then the *Status* column displays the value *down*.

Possible values:

- `0..255`
- `-`
  No tracking object of the *interface* type.

If the link to every aggregated port is interrupted, then Link aggregation, LRE and VLAN router interfaces have a negative monitoring result.

If the link to every physical port and link-aggregation interface which is a member of the VLAN is interrupted, then a VLAN router interface has a negative monitoring result.

Logical operand A

Specifies the first operand of the logical link for tracking objects of the *logical* type.

Possible values:

- Tracking objects set up
- -
  No tracking object of the *logical* type.

Logical operand B

Specifies the second operand of the logical link for tracking objects of the *logical* type.

Possible values:

- Tracking objects set up
- -
  No tracking object of the *logical* type.

Operator

Links the tracking objects specified in the *Logical operand A* and *Logical operand B* fields.

Possible values:

- *and*
  Logical AND link
- *or*
  Logical OR link
- -
  No tracking object of the *logical* type.

7.4.2 Tracking Applications

[Advanced > Tracking > Applications]

In this dialog, you see which applications are linked with the tracking objects.

The following applications can be linked with tracking objects:
- You link static routes with a tracking object in the *Routing > Routing Table* dialog, *Track name* column.
- You link virtual routers with a tracking object in the *Routing > L3-Redundancy > VRRP > Tracking* dialog. Click the button to open the *Create* window and select the tracking object from the *Track name* drop-down list.
- You link the interface status with a tracking object in the *Basic Settings > Port* dialog, *Track name* column.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 18.

Type

Displays the type of the tracking object.

Track ID

Displays the identification number of the tracking object.

Application

Displays the name of the application that is linked with the tracking object.

Possible values:
- Tracking objects of the `logical` type
- Static routes
- Virtual router of a VRRP instance
- Interface status

Track name

Displays the name of the tracking object made up of the values displayed in the *Type* and *Track ID* columns.

7.5 Command Line Interface

[Advanced > CLI]

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 an SSH-capable client application, then the SSH-capable client establishes a connection to the device management using the SSH protocol.

A Index

0-9
802.1D/p mapping . . . 285
802.1X . . . 119, 167

A
Access control . . . 167
Access control lists . . . 227
Access restriction . . . 147
ACL . . . 227
Address conflict detection . . . 32, 416
Aging time . . . 245
Alarm . . . 404
ARP . . . 416
ARP inspection . . . 217
ARP table . . . 74, 420
Audit trail . . . 492
Authentication history . . . 183
Authentication list . . . 119
Auto disable . . . 162, 163, 206, 220, 222, 339, 447, 448, 454, 476

B
Boundary clock . . . 93
Bridge . . . 336

C
CA (Certification Authority) . . . 125, 426, 436
Cable diagnosis . . . 442
Certificate . . . 23, 54, 126, 144, 145, 393, 426, 436
Certificate Revocation List (CRL) . . . 126, 426, 436
Certification Authority (CA) . . . 125, 426, 436
CLI . . . 151
Command line interface . . . 151
Community names . . . 153
Configuration check . . . 414
Configuration profile . . . 18, 50
Counter reset . . . 73
CRL (Certificate Revocation List) . . . 126, 426, 436

D
Daylight saving time . . . 76
Default gateway . . . 501
Device software . . . 45
Device software backup . . . 45
Device status . . . 21, 384
DHCP L2 Relay . . . 504
DHCP server . . . 493
DHCP snooping . . . 204
DHCPv6 L2 Relay . . . 504
Digital certificate . . . 23, 54, 126, 145, 393, 426, 436
DNS . . . 509
DNS cache . . . 510
DNS client . . . 510
Domain name system . . . 509
DoS . . . 200
DSCP . . . 287
Duplicate Address Detection . . . 40
Dynamic ARP inspection . . . 217

E
EAPOL . . . 181
Egress rate limiter . . . 247
Email notification . . . 74, 424
Encryption . . . 50
ENVM . . . 48, 55, 63, 489
Ethernet module . . . 387, 398, 400
Ethernet modules . . . 385
Event severity . . . 429, 487
External memory . . . 25, 48, 55, 63, 386, 392, 399, 489

F
Factory reset . . . 54
Fan module . . . 386, 387, 398, 401
FDB (MAC address table) . . . 73, 250
Filter MAC addresses . . . 250
Fingerprint . . . 140, 144
Flash memory . . . 48, 413
Flow control . . . 245

G
GARP . . . 277
GMRP . . . 278
Guards . . . 352
GVRP . . . 280

H
Hardware clock . . . 75
Hardware state . . . 413
HiDiscovery . . . 32, 393, 492
HIPER Ring . . . 333
Host key . . . 140
HTML . . . 412, 491
HTTP . . . 141
HTTP server . . . 391
HTTPS . . . 142

I
IAS 119, 185
IEEE 802.1X 119
IGMP snooping 74, 252
Industrial HiVision 11, 135
Ingress filtering 319
Ingress rate limiter 247
Integrated authentication server 119, 185
IP access restriction 147
IP address conflict detection 416
IP DSCP mapping 287
IP source guard 213
IPv4 rule 228

L
L2 Relay (DHCP) 504
LDAP 119
Link aggregation 357
Link backup 364
Link status 385, 398
LLDP 466
Load/save 50
Log file 73, 74, 491
Login banner 152, 155
Loop protection 400
Loops 334

M
MAC Address Conflict Detection 32
MAC flood 161
MAC rule 236
MAC spoof 163
MAC address table (forwarding database) 73, 250
Management access 32, 38, 147
Management access statistics 74
Management VLAN 32
Media redundancy protocol 329
MMRP 269
Modules 385, 386
MRP 329
MRP-IEEE 267
MRP-IEEE configuration 268
MSTP 336
MTU 69
MVRP 274

N
Network load 71
NVM 18, 48, 55

O
Out-of-band management port 42

P

Password 390
Password length 110, 390
Password policy 110
Persistent log file 74
Persistent logging 488
Port clients 179
Port configuration 172, 283
Port mirroring 458
Port monitor 454
Port priority 283
Port security 161
Port statistics 74, 181
Port VLAN 318
Port-based access control 167
Power supply 23, 387, 400
Pre-Login banner 155
Priority queue 282

Q

Queue management 289
Queues 282

R

RADIUS 119, 187
RAM 55
RAM self-test 422
Rate limiter 247
RCP 379
Reboot 73
Redundant coupling protocol 379
Relay (DHCP) 504
Request interval 85
Reset the settings 54
Ring redundancy 386, 399
Ring structure 329
Ring/Network coupling 373
RNC 373
Root bridge 336
RSTP 334, 336

S
Secure Boot 47, 394
Secure Shell (SSH) 137
Security status 22, 389
Self-test 422
Serial interface 392
Service port 42
Settings 50
Severity 429, 487
sFlow 479
SFP module 441
Signal contact 22, 395
SNMP server 135, 392
SNMP traps 69, 164, 336, 361, 384, 389, 397, 404, 418, 447, 526
SNMPv1/v2 153
SNTP 83
SNTP client 84
SNTP server 88
Software backup 45
Software update 45
Source guard 213
Spanning tree protocol 334
SSH server 137
Sub Ring redundancy 387, 400
Sub Ring 368
Support information 484
Support information (ZIP archive) 487
Syslog 435
System information 412
System log 491
System Monitor 1 422
System time 75

T
Technical Documents 537
Technical questions 537
Technical Support 537
Telnet server 136, 391
Temperature 24, 385, 398
Threshold values network load 247
Time profile 80
Topology discovery 471
Tracking 523
Training courses 537
Transparent clock 102
Trap destination 409
Traps 69, 164, 336, 361, 384, 389, 397, 404, 418, 447, 526
Trust mode 283
Twisted-pair 442

U
Unaware mode 245
Unsigned device software (allow upload) 47
Uptime 24, 413
User administration 109
Utilization 71

V

Virtual local area network 312
VLAN 34, 39, 312, 477
VLAN configuration 315
VLAN ports 318
VLAN-unaware mode 245

W

Watchdog 50, 60
Web server 141, 142

Z

ZIP archive with support information 487

B Technical 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.belden.com.

For technical support, visit my.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/services/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.

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:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
DRAGON Switch
HiOS-2A

Technical support
https://hirschmann-support.belden.com

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.

© 2026 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

Safety instructions . . . 11

About this Manual . . . 13

Key . . . 14

Replacing a device . . . 15

1 User interfaces . . . 17
1.1 Graphical User Interface . . . 17
1.1.1 System requirements . . . 17
1.1.2 Access to device management . . . 18
1.2 Command Line Interface . . . 19
1.2.1 Access to device management through the serial connection . . . 19
1.2.2 Access to the device management using SSH . . . 21
1.2.3 Mode-based command hierarchy . . . 23
1.2.4 Executing a command . . . 27
1.2.5 Structure of a command . . . 27
1.2.6 Examples of commands . . . 30
1.2.7 Input prompt . . . 31
1.2.8 Key combinations . . . 32
1.2.9 Data entry elements . . . 34
1.2.10 Use cases . . . 35
1.2.11 Service Shell . . . 36
1.3 System Monitor 1 . . . 39
1.3.1 System requirements . . . 39
1.3.2 Access to device management . . . 39
1.4 Displaying a welcome message before user login . . . 41
1.5 Displaying a welcome message after user login . . . 42

2 Specifying the IP parameters . . . 43
2.1 IP parameter basics . . . 43
2.1.1 IPv4 . . . 43
2.1.2 IPv6 . . . 47
2.2 Specifying the IP parameters using the Command Line Interface . . . 52
2.2.1 IPv4 . . . 52
2.2.2 IPv6 . . . 54
2.3 Specifying the IP parameters using HiDiscovery . . . 55
2.4 Specifying the IP parameters using the Graphical User Interface . . . 57
2.4.1 IPv4 . . . 57
2.4.2 IPv6 . . . 58
2.5 Specifying the IP parameters using BOOTP . . . 59
2.6 Specifying the IP parameters using DHCP . . . 60
2.6.1 IPv4 . . . 60
2.6.2 IPv6 . . . 61
2.7 Management address conflict detection . . . 63
2.7.1 Active and passive detection . . . 63
2.8 Duplicate Address Detection function . . . 64

3 Access to the device . . . 65
3.1 First login (Password change) . . . 65
3.2 Authentication lists . . . 66
3.2.1 Applications . . . 66
3.2.2 Policies . . . 66
3.2.3 Managing authentication lists . . . 66
3.2.4 Adjusting the settings . . . 67
3.3 User management . . . 69
3.3.1 Access roles . . . 69
3.3.2 Managing user accounts . . . 71
3.3.3 Default user accounts . . . 71
3.3.4 Changing default passwords . . . 71
3.3.5 Setting up a new user account . . . 72
3.3.6 Automatic unlocking of user accounts . . . 73
3.3.7 Deactivating the user account . . . 75
3.3.8 Adjusting policies for passwords . . . 75
3.4 LDAP function . . . 77
3.4.1 Coordination with the server administrator . . . 77
3.4.2 Setting up LDAP . . . 78
3.5 SNMP access . . . 81
3.5.1 SNMPv1/v2 access . . . 81
3.5.2 SNMPv3 access . . . 81
3.5.3 SNMPv3 traps . . . 82
3.6 Out-of-Band access . . . 85
3.6.1 Specifying the IP parameters . . . 85
3.6.2 Disabling the *Service Port* network interface . . . 87
3.7 TACACS+ . . . 88
3.7.1 Setting up a TACACS+ server entry on the device . . . 88
3.7.2 Specifying the parameters of an individual TACACS+ server entry . . . 89
3.7.3 Specifying the global parameters for every TACACS+ server entry . . . 89
3.7.4 Authenticating users through TACACS+ . . . 90
3.7.5 Authorizing commands through TACACS+ . . . 90
3.7.6 Accounting user activity on the device . . . 91

4 Synchronizing the system time in the network . . . 93
4.1 Setting the time . . . 93
4.2 Automatic daylight saving time changeover . . . 95
4.2.1 Setting daylight saving time using pre-defined profiles . . . 95
4.2.2 Setting daylight saving time manually . . . 95
4.3 Synchronizing time in the network with SNTP . . . 97
4.3.1 Preparation . . . 98
4.3.2 Defining settings of the SNTP client . . . 98
4.3.3 Specifying SNTP server settings . . . 100
4.4 Synchronizing time in the network with PTP . . . 101
4.4.1 Types of clocks . . . 101
4.4.2 Best Master Clock algorithm . . . 102
4.4.3 Delay measurement . . . 102
4.4.4 PTP domains . . . 103
4.4.5 Using PTP . . . 103
4.4.6 Selecting the ports used for PTP . . . 104

5 Managing configuration profiles . . . 105
5.1 Detecting changed settings . . . 105
5.1.1 Volatile memory (RAM) and non-volatile memory (NVM). . . . 105
5.1.2 external memory (ENVM) and non-volatile memory (NVM) . . . 106
5.2 Saving the settings . . . 107
5.2.1 Saving the configuration profile in the device . . . 107
5.2.2 Saving the configuration profile in the external memory (ENVM) . . . 109
5.2.3 Backing up the configuration profile on a remote server . . . 109
5.2.4 Exporting a configuration profile . . . 110
5.3 Loading settings . . . 112
5.3.1 Activating a configuration profile . . . 112
5.3.2 Loading the configuration profile from the external memory (ENVM) . . . 112
5.3.3 Importing a configuration profile . . . 114
5.4 Resetting the device to the default setting . . . 117
5.4.1 Using the Graphical User Interface or Command Line Interface . . . 117
5.4.2 Using System Monitor 1 . . . 117

6 Updating the device software . . . 119
6.1 Loading a previous device software version . . . 119
6.2 Software update from the PC . . . 120
6.3 Software update from a server . . . 121
6.3.1 Software update through FTP . . . 121
6.3.2 Software update through TFTP . . . 122
6.3.3 Software update through SFTP . . . 123
6.3.4 Software update through SCP . . . 125
6.4 Software update from the external memory (ENVM) . . . 127
6.4.1 Manually—initiated by the administrator . . . 127
6.4.2 Automatically—initiated by the device . . . 127

7 Configuring the ports . . . 129
7.1 Enabling/Disabling the port . . . 129
7.2 Selecting the operating mode . . . 130
7.3 Gigabit Ethernet mode for ports . . . 131
7.3.1 Checking port parameters . . . 131

8 Assistance in the protection from unauthorized access . . . 133
8.1 Changing the SNMPv1/v2 community . . . 133
8.2 Disabling write access for SNMPv1/v2 . . . 134
8.3 Disabling SNMPv1/v2 . . . 135
8.4 Disabling HTTP . . . 136
8.5 Disabling Telnet . . . 137
8.6 Disabling the HiDiscovery access . . . 138
8.7 Restricting access to device management . . . 139
8.7.1 Restricting access from a specific IP address range . . . 139
8.8 Adjusting the session timeouts . . . 141
8.9 Deactivating the unused modules . . . 143
8.10 Customizing the SSH settings . . . 144
8.10.1 Generating the RSA host key in the device . . . 144
8.10.2 Transferring an externally generated private RSA key to the device . . . 145
8.11 Making SSH hosts known to the device . . . 148

9	**Controlling the data traffic**	151
9.1	Helping protect against DoS attacks	151
9.1.1	Filters for TCP and UDP packets	152
9.1.2	Filters for IP packets	156
9.1.3	Filters for ICMP packets	156
9.2	ACL	159
9.2.1	Creating and editing IPv4 rules	160
9.2.2	Creating and configuring an IP ACL using the Command Line Interface	162
9.2.3	Creating and editing MAC rules	162
9.2.4	Creating and configuring a MAC ACL using the Command Line Interface	163
9.2.5	Assigning ACLs to a port or VLAN	164
9.2.6	Maximum number of rules that can be assigned	164
9.3	MAC authentication bypass	166
10	**Network load control**	167
10.1	Direct packet distribution	167
10.1.1	Learning MAC addresses	167
10.1.2	Aging of learned MAC addresses	167
10.1.3	Static address entries	168
10.2	Multicasts	171
10.2.1	Example of a Multicast application	171
10.2.2	IGMP snooping	171
10.3	Rate limiter	176
10.4	QoS/Priority	177
10.4.1	Description of prioritization	177
10.4.2	Handling of received priority information	178
10.4.3	VLAN tagging	178
10.4.4	IP ToS (Type of Service)	179
10.4.5	Handling of traffic classes	180
10.4.6	Queue management	181
10.4.7	Management prioritization	183
10.4.8	Setting prioritization	184
10.5	Differentiated services	188
10.5.1	Application example for the DiffServ function	189
10.6	Flow control	191
10.6.1	Flow Control with a full-duplex link	191
10.6.2	Setting up the Flow Control	192
11	**VLANs**	193
11.1	Examples of VLANs	193
11.1.1	Application example of a simple port-based VLAN	194
11.1.2	Application example of a complex VLAN setup	198
11.2	Guest VLAN / Unauthenticated VLAN	203
11.3	RADIUS VLAN assignment	205
11.4	Creating a Voice VLAN	206
11.5	MAC based VLANs	207
11.6	IP subnet-based VLANs	208
11.7	Protocol-based VLAN	209
11.8	VLAN unaware mode	210

12 Redundancy . . . 211
12.1 Network Topology vs. Redundancy Protocols . . . 211
12.1.1 Network topologies . . . 211
12.1.2 Redundancy Protocols . . . 213
12.1.3 Combinations of redundancy protocols . . . 213
12.2 Media Redundancy Protocol (MRP) . . . 215
12.2.1 Network structure . . . 215
12.2.2 Reconfiguration time . . . 216
12.2.3 Advanced mode . . . 216
12.2.4 Prerequisites for MRP . . . 216
12.2.5 Advanced Information . . . 217
12.2.6 Application example of an MRP Ring . . . 218
12.2.7 MRP over LAG . . . 222
12.3 HIPER Ring Client . . . 226
12.3.1 VLANS on the HIPER Ring . . . 226
12.3.2 Advanced Information . . . 227
12.3.3 HIPER Ring over LAG . . . 228
12.4 Spanning Tree . . . 229
12.4.1 Basics . . . 229
12.4.2 Rules for Creating the Tree Structure . . . 233
12.4.3 Examples . . . 235
12.5 Rapid Spanning Tree Protocol . . . 238
12.5.1 Port roles . . . 238
12.5.2 Port states . . . 239
12.5.3 Spanning Tree Priority Vector . . . 240
12.5.4 Fast reconfiguration . . . 240
12.5.5 Configuring the device . . . 241
12.5.6 Guards . . . 243
12.5.7 Ring only mode function . . . 246
12.6 Link Aggregation . . . 248
12.6.1 Methods of Operation . . . 248
12.6.2 Link Aggregation Example . . . 249
12.7 Link Backup . . . 250
12.7.1 Fail Back Description . . . 250
12.7.2 Application example for the Link Backup function . . . 250
12.8 FuseNet function . . . 253
12.9 Sub Ring . . . 254
12.9.1 Sub Ring description . . . 254
12.9.2 Advanced Information . . . 256
12.9.3 Sub Ring example . . . 257
12.9.4 Application example for the Sub Ring function . . . 259
12.9.5 Cascaded Sub Rings example . . . 260
12.9.6 Sub Ring with LAG . . . 263
12.10 Ring/Network Coupling function . . . 267
12.10.1 Methods of Ring/Network Coupling . . . 267
12.10.2 Advanced Information . . . 269
12.10.3 Prepare the Ring/Network Coupling . . . 274
12.11 RCP function . . . 287
12.11.1 Prerequisites for RCP . . . 289
12.11.2 Advanced Information . . . 289
12.11.3 Application example for RCP coupling . . . 290

13 Tracking . . . 295
13.1 Interface tracking . . . 295
13.2 Logical tracking . . . 297
13.3 Configuring the tracking . . . 298
13.3.1 Configuring interface tracking . . . 298
13.4 Interface status application . . . 300
13.4.1 Special conditions during use . . . 300
13.4.2 Example for the Interface status application . . . 300

14 Operation diagnosis . . . 303
14.1 Sending SNMP traps . . . 303
14.1.1 SNMP traps for configuration activity . . . 303
14.1.2 SNMP trap setting . . . 304
14.1.3 ICMP messaging . . . 304
14.2 Monitoring the Device Status . . . 305
14.2.1 Events which can be monitored . . . 305
14.2.2 Configuring the Device Status . . . 306
14.2.3 Displaying the Device Status . . . 308
14.3 Security Status . . . 309
14.3.1 Events which can be monitored . . . 309
14.3.2 Configuring the Security Status . . . 310
14.3.3 Displaying the Security Status . . . 312
14.4 Out-of-Band signaling . . . 313
14.4.1 Controlling the Signal contact . . . 313
14.4.2 Monitoring the Device and Security Statuses . . . 314
14.5 Port event counter . . . 317
14.5.1 Detecting non-matching duplex modes . . . 317
14.6 Auto-Disable . . . 319
14.7 Displaying the SFP status . . . 321
14.8 Topology discovery . . . 322
14.8.1 Displaying the Topology discovery results . . . 322
14.8.2 LLDP-Med . . . 323
14.9 Detecting loops . . . 324
14.10 Helping avoid layer 2 network loops . . . 325
14.10.1 Helping avoid layer 2 network loops . . . 325
14.10.2 Recommendations for redundant ports . . . 327
14.11 Using the Email Notification function . . . 328
14.11.1 Specifying the sender address . . . 328
14.11.2 Specifying the triggering events . . . 328
14.11.3 Changing the sending interval . . . 329
14.11.4 Specifying the recipients . . . 330
14.11.5 Specifying the mail server . . . 330
14.11.6 Enabling/Disabling the Email Notification function . . . 331
14.11.7 Sending a test email . . . 331
14.12 Reports . . . 333
14.12.1 Global settings . . . 333
14.12.2 Syslog . . . 335
14.12.3 System Log . . . 336
14.12.4 Syslog over TLS . . . 338
14.12.5 Audit Trail . . . 339
14.13 Network analysis with TCPdump . . . 340

14.14 Monitoring the data stream with Port Mirroring . . . 341
14.14.1 Enabling the Port Mirroring function . . . 342
14.15 Monitoring the data stream with VLAN mirroring . . . 343
14.15.1 Application example for the VLAN mirroring function . . . 343
14.16 Monitoring data streams with RSPAN . . . 345
14.16.1 Purpose . . . 345
14.16.2 RSPAN topologies . . . 345
14.16.3 RSPAN VLAN properties . . . 348
14.16.4 RSPAN device roles . . . 349
14.16.5 RSPAN uplinks . . . 351
14.16.6 Reflector port on a source device . . . 351
14.16.7 Use of underlying redundancy protocols . . . 352
14.16.8 Packet prioritization . . . 353
14.16.9 Starting point for the examples . . . 354
14.16.10 Example: RSPAN with a reflector port . . . 354
14.16.11 Example: RSPAN without a reflector port . . . 358
14.17 Self-test . . . 361
14.18 Copper cable test . . . 363
14.19 Network monitoring with sFlow . . . 364

15 Advanced functions of the device . . . 367
15.1 DHCP server . . . 367
15.1.1 Settings that the server assigns to the clients . . . 367
15.1.2 Pools . . . 367
15.1.3 Setting up a Preboot eXecution Environment (PXE) . . . 370
15.2 DHCP L2 Relay . . . 372
15.2.1 Circuit and Remote IDs . . . 372
15.2.2 DHCP L2 Relay configuration . . . 373
15.3 Using the device as a DNS client . . . 376
15.3.1 Setting up the DNS client function . . . 376
15.3.2 Setting up a static host . . . 377
15.4 GARP function . . . 378
15.4.1 Configuring GMRP . . . 378
15.4.2 Configuring GVRP . . . 379
15.5 MRP-IEEE . . . 380
15.5.1 MRP-IEEE operation . . . 380
15.5.2 MRP-IEEE timers . . . 380
15.5.3 MMRP . . . 381
15.5.4 MVRP . . . 383

16 Industry Protocols . . . 385
16.1 OPC UA Server . . . 386
16.1.1 Enabling the OPC UA server . . . 389
16.1.2 Setting up an OPC UA user account . . . 390
16.1.3 Deactivating an OPC UA user account . . . 391
16.1.4 Deleting an OPC UA user account . . . 391
16.2 Service Discovery . . . 393
16.2.1 ITxPT Module Inventory . . . 393
16.2.2 Application example . . . 394

A Setting up the configuration environment . . . 397
A.1 Setting up a DHCP/BOOTP server . . . 397
A.2 Setting up a DHCP server with Option 82 . . . 400

A.3 HTTPS certificate . . . 403
A.3.1 Conflicts in certificate validation . . . 403
A.3.2 HTTPS certificate management . . . 403
A.3.3 Access through HTTPS . . . 404

B Appendix . . . 407
B.1 Literature references . . . 407
B.2 Management Information Base (MIB) . . . 408
B.3 List of RFCs . . . 410
B.4 Underlying IEEE Standards . . . 413
B.5 Underlying IEC Norms . . . 414
B.6 Underlying ANSI Norms . . . 415
B.7 Technical Data . . . 416
B.7.1 Switching . . . 416
B.7.2 VLAN . . . 416
B.7.3 Access Control Lists (ACL) . . . 416
B.8 Copyright of integrated Software . . . 417
B.9 Abbreviations used . . . 418

C Index . . . 421

D Technical support . . . 429

E Readers' Comments . . . 430

Safety instructions

⚠ WARNING

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, which is available in English only, contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Security” user manual, which is available in English only, introduces system security planning and policy development. It provides a detailed list of device security measures. It also describes how a secured device can improve the security and availability of your network. Its appendix contains details on hardware security seals and a password strength policy guide.

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:

•	List item
–	List item – second level
▶	Parameter value
☐	Task 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

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 (*ENVM*).
  See “Loading the configuration profile from the external memory (ENVM)” on page 112.
- The new device gets its IP address using DHCP *Option 82*.
  See “DHCP L2 Relay” on page 372.
  See “Setting up a DHCP server with Option 82” on page 400.

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 transfer your own digital certificate onto the device.
  See “HTTPS certificate management” on page 403.
- 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 “Transferring an externally generated private RSA key to the device” on page 145.

1 User interfaces

The device lets you access the device management through the following user interfaces.

User interface	Requires Authorization	Accessible through …	Prerequisite
Graphical User Interface	Yes	Ethernet	Web browser
Command Line Interface	Yes	Ethernet	SSH client
		Serial interface	VT100 terminal emulation
System Monitor 1	No	Serial interface	

Authorization to access the device management is assigned in the following ways:
- With a user account set up on the device
  See “User management” on page 69.
- A remote server grants authorization
  - RADIUS
  - LDAP, see “LDAP function” on page 77
  - TACACS+, see “TACACS+” on page 88

This chapter contains the following topics:
▶ Graphical User Interface
▶ Command Line Interface
▶ System Monitor 1
▶ Displaying a welcome message before user login
▶ Displaying a welcome message after user login

1.1 Graphical User Interface

1.1.1 System requirements

To access the device management using the the Graphical User Interface, you need a web browser with HTML5 support.

Web browsers and other third-party software routinely validate digital certificates. If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:
- ☐ Verify if the digital certificate of the device has expired.
- ☐ Verify if your web browser no longer regards the algorithm used for generating the digital certificate as trustworthy.

To solve the conflict in validation, regenerate the digital certificate on the device using the latest device software. As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device.

1.1.2 Access to device management

The prerequisite for accessing the device management is that the IP parameters are set up in the device. See “Specifying the IP parameters” on page 43.

Perform the following steps:

- ☐ Start the web browser on the management station.
- ☐ Type the IP address of the device in the address field of the web browser.
  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 and password.
  - –
  - – The default user name is `admin`.
  - – The default password is `private`.
    When you enter the default password during the initial setup of the device, the device will prompt you to enter a new password.
    See “First login (Password change)” on page 65.
- ☐ Click the *Login* button.
  If the device accepts the credentials you entered, you are logged in to the device management.

1.2 Command Line Interface

The Command Line Interface provides IT specialists with a familiar environment for configuring IT devices. As an experienced user or administrator, you know the network basics and how to operate Hirschmann devices.

You can access the device management using the Command Line Interface in the following ways:
- Through the serial connection
  See “Access to device management through the serial connection” on page 19.
- Over the network using Secure Shell (SSH)
  See “Access to the device management using SSH” on page 21.

You find information about assembling and starting up the device in the “Installation” user manual.

1.2.1 Access to device management through the serial connection

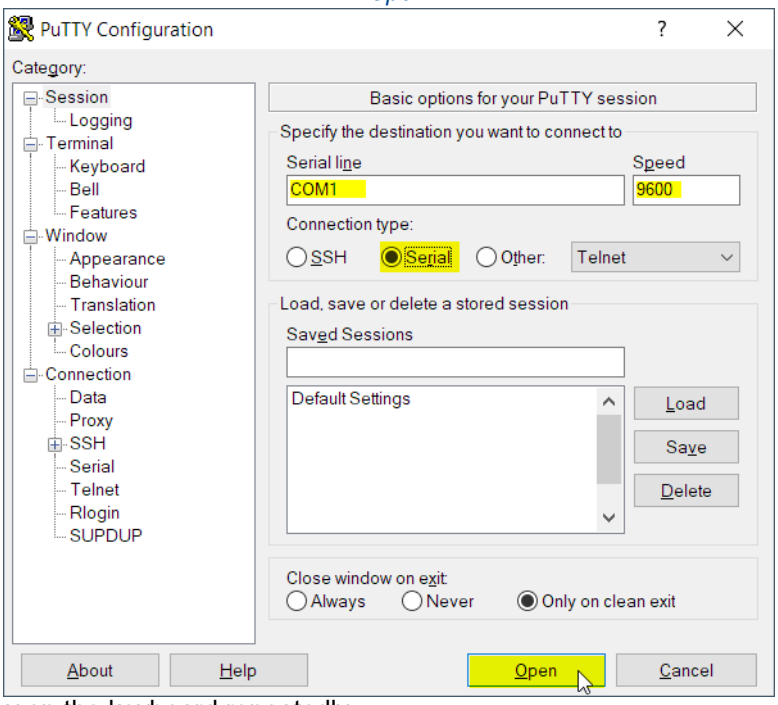
To access the device management, connect a management station with VT100 terminal emulation to the serial interface of the device.

VT100 terminal emulation settings	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Parity	None
Handshake	None

The following example guides you through the necessary steps using the *PuTTY* application as VT100 terminal emulation. You can download the *PuTTY* application from www.chiark.greenend.org.uk/~sgtatham/putty/.

Perform the following steps:
- ☐ Connect the management station to the serial interface of the device.
- ☐ On the management station, start the VT100 terminal emulation.

☐ Set up the serial connection. Then click the *Open* button.



☐ Press any key on the keyboard repeatedly.
After a few seconds, the VT100 terminal emulation displays the login screen.

☐ Enter the user name and password.
- The default user name is `admin`.
- The default password is `private`.
  When you enter the default password during the initial setup of the device, the device will prompt you to enter a new password. See “First login (Password change)” on page 65.

You are logged in to the device management.

```
                    Copyright (c) 2011-2026 Hirschmann Automation and Control GmbH

                                    All rights reserved

                                DRAGON-00484 Release HiOS-2A-10.6.00

                                   (Build date 2026-10-03 09:34)


                    System Name   :  DRAGON-ECE555d6e976
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    OOB IP        :  192.168.1.1
                    OOB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:45:49


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.

DRAGON>
```

Figure 1: Start screen of the Command Line Interface

1.2.2 Access to the device management using SSH

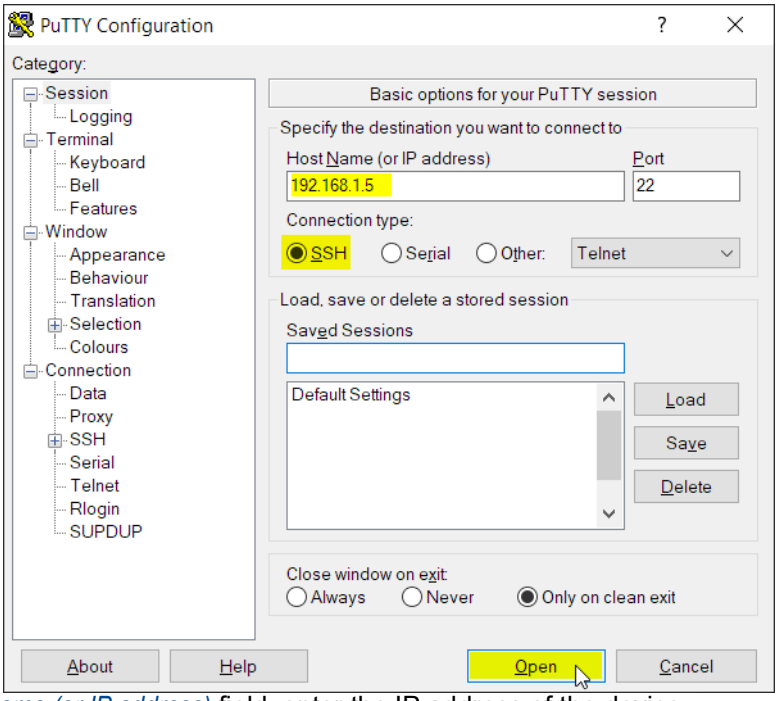
The prerequisite for accessing the device management is that the IP parameters are set up in the device. See “Specifying the IP parameters” on page 43.

The following example guides you through the necessary steps using the *PuTTY* application as the SSH client. You can download the *PuTTY* application from www.chiark.greenend.org.uk/~sgtatham/putty/. As an alternative, you can use the `ssh` command, which is part of OpenSSH.

Perform the following steps:

- ☐ Connect the management station to the device over the Ethernet network.
- ☐ On the management station, start the SSH client application.

☐ Set up the SSH connection.

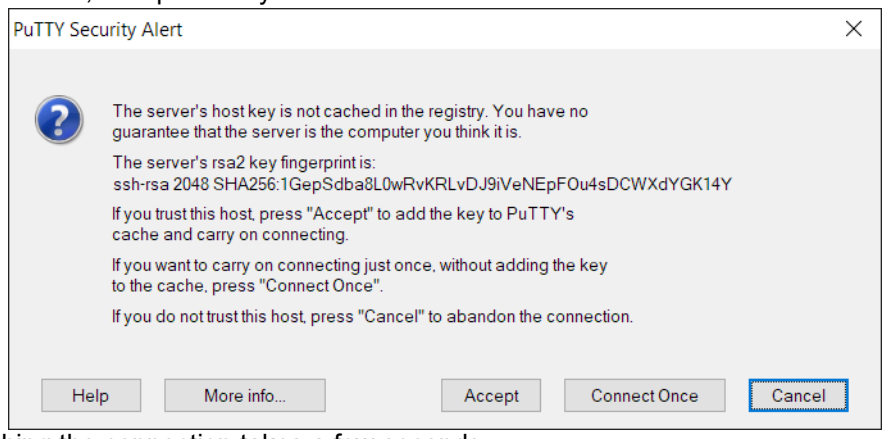


☐ In the *Host Name (or IP address)* field, enter the IP address of the device.
☐ In the *Connection type* option list, select the *SSH* radio button.
☐ Click the *Open* button.
When you connect the management station to the device for the first time, the SSH client application displays a *host key* verification message.

☐ Check the fingerprint of the key the SSH server of the device sends.

Note:
On the device, you can display the fingerprint of the *host key* with the command `show ssh server` or in the *Device Security > Management Access > Server* dialog, *SSH* tab.

☐ To continue, accept the key.



Establishing the connection takes a few seconds.

☐ Enter the user name and password.
– The default user name is `admin`.
– The default password is `private`.
When you enter the default password during the initial setup of the device, the device will prompt you to enter a new password. See “First login (Password change)” on page 65.

You are logged in to the device management.

```
login as: admin
admin@192.168.1.5's password:


                    Copyright (c) 2011-2026 Hirschmann Automation and Control GmbH

                                  All rights reserved

                              DRAGON-00484 Release HiOS-2A-10.6.00

                                 (Build date 2026-10-03 09:34)


                    System Name   :  DRAGON-ECE555d6e976
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    OOB IP        :  192.168.1.1
                    OOB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:45:49


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.

DRAGON>
```

Figure 2: Start screen of the Command Line Interface

1.2.3 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.

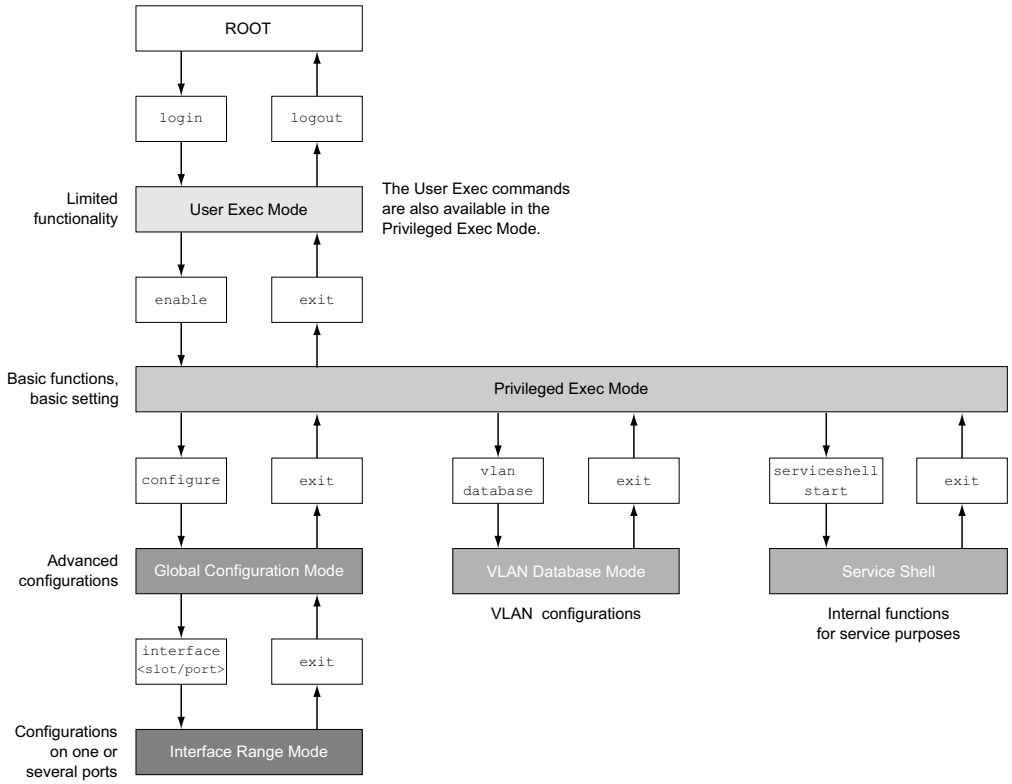


Figure 3: Structure of the Command Line Interface

The Command Line Interface supports, depending on the user level, the following modes:

- *User Exec* mode
  When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The *User Exec* mode contains a limited range of commands.
  Command prompt: `(DRAGON) >`
- *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 into the device management as a privileged user. In the *Privileged Exec* mode, you are able to execute the *User Exec* mode commands, too.
  Command prompt: `(DRAGON) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(DRAGON) (VLAN)#`
- Service Shell
  The Service Shell is for service purposes only.
  Command prompt: `/mnt/fastpath #`

- *Global Config* mode
  The *Global Config* mode lets you perform modifications to the current configuration. This mode groups general setup commands.
  Command prompt: `(DRAGON) (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: `(DRAGON) ((interface) all)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface all
    (DRAGON) ((Interface)all)#
    ```
  - A single port on one interface
    Command prompt: `(DRAGON) (interface <slot/port>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 2/1
    (DRAGON) (interface 2/1)#
    ```
  - A range of ports on one interface
    Command prompt: `(DRAGON) (interface <interface range> )#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2-1/4
    (DRAGON) ((Interface)1/2-1/4)#
    ```
  - A list of single ports
    Command prompt: `(DRAGON) (interface <interface list>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2,1/4,1/5
    (DRAGON) ((Interface)1/2,1/4,1/5)#
    ```
  - A list of port ranges and single ports
    Command prompt: `(DRAGON) (interface <complex range>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (DRAGON) (config)#interface 1/2-1/4,1/6-1/9
    (DRAGON) ((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 1: Command modes

Command mode	Access method	Quit or start next mode

User Exec mode	First access level. Perform basic tasks and list system information.	To quit you enter `logout`:
		`(DRAGON) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec mode	From the *User Exec* mode, you enter the command `enable`:
	`(DRAGON) >enable`
	`(DRAGON) #`
		To quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit`:
		`(DRAGON) #exit`
		`(DRAGON) >`

Table 1: Command modes

Command mode	Access method	Quit or start next mode

VLAN mode	From the *Privileged Exec* mode, you enter the command `vlan database`:
	`(DRAGON) #vlan database`
	`(DRAGON) (Vlan)#`
		To end the VLAN mode and return to the *Privileged Exec* mode, you enter `exit` or press <CTRL>+<Z>.
		`(DRAGON) (Vlan)#exit`
		`(DRAGON) #`

Global Config mode	From the *Privileged Exec* mode, you enter the command `configure`:
	`(DRAGON) #configure`
	`(DRAGON) (config)#`
	From the *User Exec* mode, you enter the command `enable`, and then in *Privileged Exec* mode, enter the command `Configure`:
	`(DRAGON) >enable`
	`(DRAGON) #configure`
	`(DRAGON) (config)#`
		To quit the *Global Config* mode and return to the *Privileged Exec* mode, you enter `exit`:
		`(DRAGON) (config)#exit`
		`(DRAGON) #`
		To then quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit` again:
		`(DRAGON) #exit`
		`(DRAGON) >`

Interface Range mode	From the *Global Config* mode you enter the command `interface {all|<slot/port>|<interface range>|<interface list>|<complex range>}`.
	`(DRAGON) (config)#interface <slot/port>`
	`(DRAGON) (interface slot/port)#`
		To quit the *Interface Range* mode and return to the *Global Config* mode, you enter `exit`. To return to the *Privileged Exec* mode, you press <CTRL>+<Z>.
		`(DRAGON) (interface slot/port)#exit`
		`(DRAGON) #`

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.

```
(DRAGON)>
  cli             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.

(DRAGON)>
```

Figure 4: Commands in the User Exec mode

1.2.4 Executing a command

Syntax analysis

When you log into the device management with the Command Line Interface, you are in the *User Exec* mode. The Command Line Interface displays the prompt `(DRAGON)>` 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:

```
(DRAGON)>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.

1.2.5 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 2: Parameter and command syntax

`<command>`	Commands in pointed brackets (<>) are obligatory.
`[command]`	Commands in square brackets ([]) are optional.
`<parameter>`	Parameters in pointed brackets (<>) are obligatory.
`[parameter]`	Parameters in square brackets ([]) are optional.
`...`	An ellipsis (3 points in sequence without spaces) after an element indicates that you can repeat the element.
`[Choice1 | Choice2]`	A vertical line enclosed in brackets indicates a selection option. Select one value. Elements separated by a vertical line and enclosed in square brackets indicate an optional selection (Option1 or Option2 or no selection).
`{list}`	Curved brackets ({}) indicate that a parameter is to be selected from a list of options.
`{Choice1 | Choice2}`	Elements separated by a vertical line and enclosed in curved brackets ({}) indicate an obligatory selection option (option1 or option2).
`[param1 {Choice1 | Choice2}]`	Displays an optional parameter that contains an obligatory selection.
`<a.b.c.d>`	Small letters are wild cards. You enter parameters with the notation a.b.c.d with decimal points (for example IP addresses)
`<cr>`	You press the <Enter> key to insert a line break (carriage return).

The following list displays the possible parameter values within the Command Line Interface:

Table 3: Parameter values in the Command Line Interface

Value	Description
IP address	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.
MAC address	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`.
string	User-defined text with a length in the specified range, for example a maximum of 32 characters.

Table 3: Parameter values in the Command Line Interface

Value	Description
character string	Use double quotation marks to indicate a character string, for example “System name with space character”.
number	Whole integer in the specified range, for example 0..999999.
date	Date in format YYYY-MM-DD.
time	Time in format HH:MM:SS.

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 4: Format and range of network addresses

Address Type	Format	Range	Example
IP address	nnn.nnn.nnn.nnn	nnn: 0 to 255 (decimal)	192.168.11.110
MAC address	mm:mm:mm:mm:mm:mm	mm: 00 to ff (hexadecimal number pairs)	A7:C9:89:DD:A9:B3

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:

```
*(DRAGON)#cli prompt Device name
Error: Invalid command 'name'

*(DRAGON)#cli prompt 'Device name'

*(Device name)#
```

1.2.6 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 specify the RADIUS server timeout value.

```
(DRAGON) (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.

```
(DRAGON) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
                      (default: 1812).
 [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.

1.2.7 Input prompt

Command mode

With the input prompt, the Command Line Interface displays which of the three modes you are in:

- `(DRAGON) >`
  User Exec mode
- `(DRAGON) #`
  Privileged Exec mode
- `(DRAGON) (config)#`
  Global Config mode
- `(DRAGON) (Vlan)#`
  VLAN Database mode
- `(DRAGON) ((Interface)all)#`
  Interface Range mode / All ports of the device
- `(DRAGON) ((Interface)2/1)#`
  Interface Range mode / A single port on one interface
- `(DRAGON) ((Interface)1/2-1/4)#`
  Interface Range mode / A range of ports on one interface
- `(DRAGON) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / A list of single ports
- `(DRAGON) ((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.
  `*(DRAGON)>`
- 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.
  `*#(DRAGON)>`
- 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.
  `!(DRAGON)>`

Wildcards

The device lets you change the command line prompt.

The Command Line Interface supports the following wildcards:

Table 5: Using wildcards within the Command Line Interface input prompt

Wildcard	Description
`%d`	System date
`%t`	System time

Table 5: Using wildcards within the Command Line Interface input prompt

Wildcard	Description
%i	IP address of the device
%m	MAC address of the device
%p	Product name of the device

```
!(DRAGON)>enable

!(DRAGON)#cli prompt %i

!192.168.1.5#cli prompt (DRAGON)%d

!*(DRAGON)2026-10-05#cli prompt (DRAGON)%d%t

!*(DRAGON)2026-10-05 12:45:49#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.8 Key combinations

The following key combinations make it easier for you to work with the Command Line Interface:

Table 6: Key combinations in the Command Line Interface

Key combination	Description
<CTRL> + <H>, <Backspace>	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>	Rewrite or paste 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

The Help command displays the possible key combinations in Command Line Interface on the screen:

```
(DRAGON) #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

(DRAGON) #
```

Figure 5: Listing the key combinations with the Help command

1.2.9 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:
  ```
  (DRAGON) (Config)#lo
  (DRAGON) (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 `(DRAGON) >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:

```
!*#(DRAGON)(Config)#show?

   show          Display device options and settings.
```

1.2.10 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:

- ☐ Enter `enable` to change to the *Privileged Exec* mode.
- ☐ Enter the following command:
  `save [profile]`
- ☐ 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`).

Parameter	Meaning	Possible values
`<1..8>`	RADIUS server index.	`1..8`
`<a.b.c.d>`	RADIUS accounting server IP address.	IP address
`<string>`	Enter a user-defined text, max. 32 characters.	
`<1..65535>`	Enter port number between 1 and 65535.	`1..65535`

Mode and Privilege Level:

- Prerequisites for executing the command:
  - You are in the *Global Config* mode.
    See “Mode-based command hierarchy” on page 23.
  - You have the access role *administrator*.

Syntax of commands and parameters: See “Structure of a command” on page 27.

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`

1.2.11 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 inoperable device**.

Start the Service Shell

The prerequisite is that you are in *User Exec* mode: `(DRAGON) >`

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.

```
!DRAGON >enable

!*DRAGON #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 (2026-10-05 12:45:49 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. **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: `(DRAGON) >`

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.

```
!DRAGON >enable

!*DRAGON #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 1

The System Monitor 1 provides functions for recovering the operating settings of the device. If the option of accessing System Monitor 1 during system startup is active, see the *Diagnostics > System >* Selftest dialog, you can start the System Monitor 1 during system startup. The prerequisite is that the management station is connected to the device through the serial connection.

In System Monitor 1, you carry out the following tasks, for example:
- Managing the operating system and verifying the device software image
- Starting the operating system
- Deleting configuration profiles, resetting the device to the factory settings
- Checking boot code information

1.3.1 System requirements

To access the device management, connect a management station with VT100 terminal emulation to the serial interface of the device.

VT100 terminal emulation settings	
Speed	`9600 bit/s`
Data	`8 bit`
Stopbit	`1 bit`
Parity	`None`
Handshake	`None`

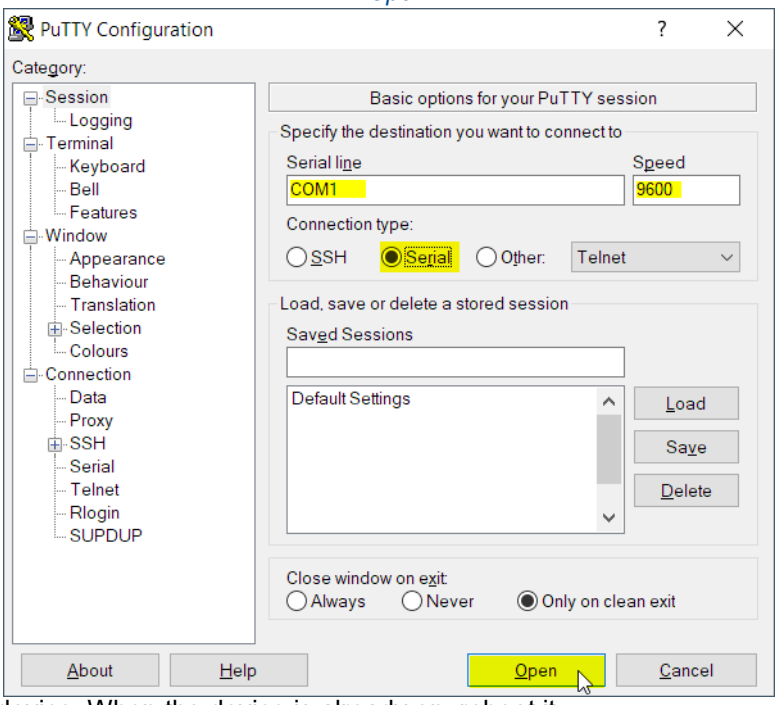
1.3.2 Access to device management

The following example guides you through the necessary steps using the *PuTTY* application as VT100 terminal emulation. You can download the *PuTTY* application from www.chiark.greenend.org.uk/~sgtatham/putty/.

Required accessories:
- Terminal cable for connecting the management station to the device (optional accessory)
- Management station with VT100 terminal emulation

Perform the following steps:
- ☐ Connect the management station to the serial interface of the device.
- ☐ On the management station, start the VT100 terminal emulation.

☐ Set up the serial connection. Then click the *Open* button.



☐ Turn on the device. When the device is already on, reboot it.
During system startup, the VT100 terminal emulation displays the following line:

```
Press <1> to change to System Monitor 1.
```

☐ Press the <1> key within 3 seconds.
The device starts the System Monitor 1.
The VT100 terminal emulation displays the following view:

```
System Monitor 1
(Selected OS: ...-10.6 (2026-10-03 09:34))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

☐ Select a menu item by entering the number.
☐ To leave a submenu and return to the main menu, press the <ESC> key.

1.4 Displaying a welcome message before user login

You can set up a welcome message that the device displays before a user logs in to the device management.

Independently of this, you can also set up a post-login welcome message. The device displays the post-login welcome message after a user logs in to the device management using the Command Line Interface. See “Displaying a welcome message after user login” on page 42.

For security reasons, enter only the minimum necessary information. Avoid any information that might help an unauthorized user. In case of doubt, find a reasonable compromise based on your security policy.

The following example demonstrates how to set up the pre-login welcome message.

Perform the following steps:

- ☐ Open the *Device Security > Pre-login Banner* dialog.
- ☐ In the *Banner text* field, enter the desired string, for example, `Welcome! You need certain permissions to access the device management.`
- ☐ Enable the *Pre-login Banner* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`system pre-login-banner text "Welcome! You need certain permissions to access the device management."`	To specify the string that the device displays before a user logs in to the device management. Enclose the string in quotation marks. The device will display the string without the quotation marks.
`system pre-login-banner operation`	To enable the pre-login banner function.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

1.5 Displaying a welcome message after user login

You can set up a welcome message that the device displays after a user logs in to the device management using the Command Line Interface.

Independently of this, you can also set up a pre-login welcome message. The device displays the pre-login welcome message before a user logs in to the device management. See “Displaying a welcome message before user login” on page 41.

The following example demonstrates how to set up the post-login welcome message.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > CLI* dialog, *Login banner* tab.
- ☐ In the *Banner text* field, enter the desired string, for example, `Welcome to the Command Line Interface!`.
- ☐ Enable the *Login banner* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`cli banner text "Welcome to the Command Line Interface!"`	To specify the string that the device displays after a user logs in to the device management. Enclose the string in quotation marks. The device will display the string without the quotation marks.
`cli banner operation`	To enable the post-login banner function.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

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 (*ENVM*), you choose this method.
- Using BOOTP.
  To set up the installed device to use 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 the MAC address of the device. The DHCP mode is the default mode for the configuration data reference.
- Configuration using DHCP.
  To set up the installed device to use 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 the MAC address or the system name of the device.
- 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 7: IP address classes

Class	Network address	Host address	Address range
A	1 Byte	3 Bytes	0.0.0.0..127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0..191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0..223.255.255.255
D			224.0.0.0..239.255.255.255
E			240.0.0.0..255.255.255.255

The first byte of an IP address is the network address. The worldwide leading regulatory board for assigning network addresses is the Internet Assigned Numbers Authority (IANA). 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

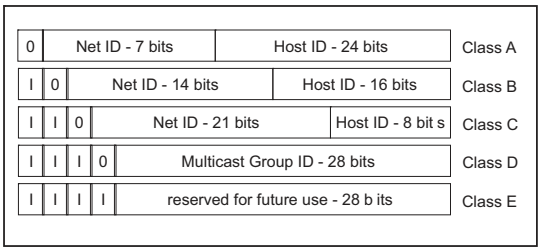


Figure 6: Bit representation of the IP address

When the first bit of an IP address is 0, it belongs to class A. The first octet is less than 128.

When the first bit of an IP address is 1 and the second bit is 0, it belongs to class B. The first octet is between 128 and 191.

When the first 2 bits of an IP address are 1, it belongs to class C. The first octet is higher than 191.

Assigning the address of the host (*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 subnets. The netmask assigns the IP addresses of the individual devices to a particular subnet.

You perform subnet 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 subnet 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

How to use the netmask

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?

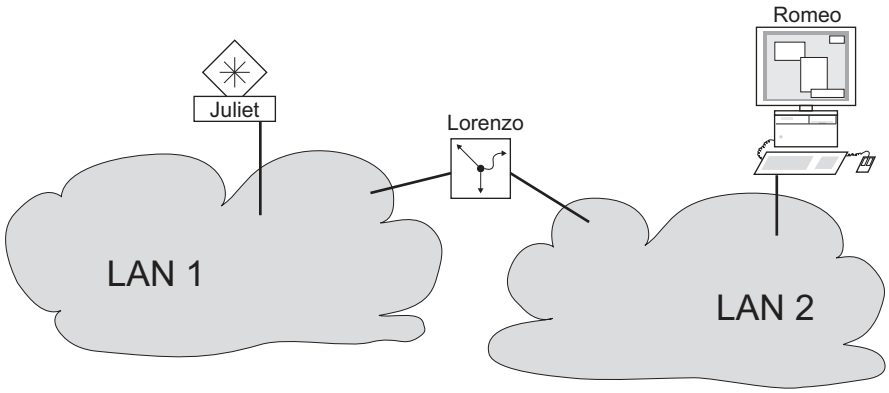


Figure 7: The management agent is separated from its network management station by a router

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 (2^8-2) addresses was too small, and class B with a maximum of 65534 $(2^{16}-2)$ 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:

IP address, decimal	Network mask, decimal	IP address, binary
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111

25 mask bits

CIDR notation: 192.168.112.0/25

Mask bits

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: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.

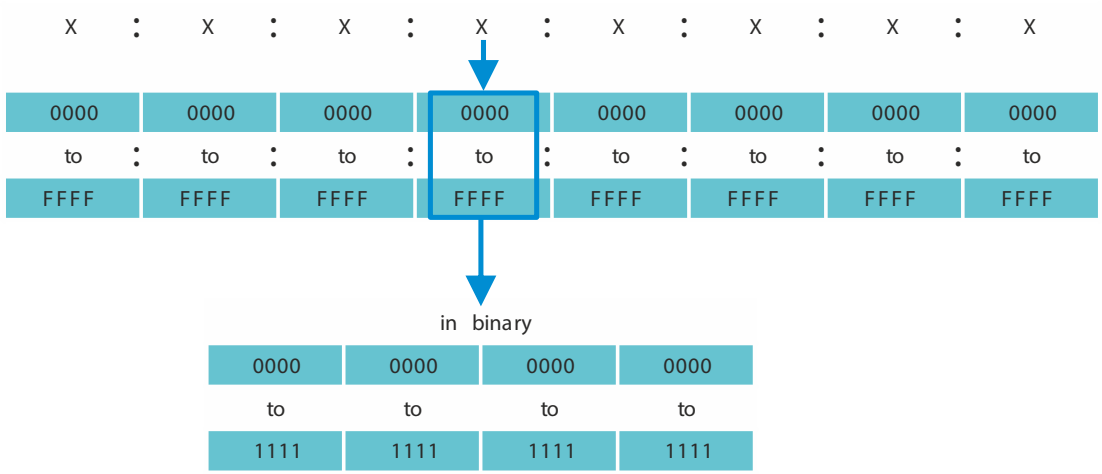


Figure 8: IPv6 address representation

As you can see in the figure above, usually an IPv6 address contains many zeros. 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 8: IPv6 address compression

Preferred	CC03:0000:0000:0000:0001:AB30:0400:FF02
No leading zeros	CC03: 0: 0: 0: 1:AB30: 400:FF02
Compressed	CC03::1:AB30:400:FF02

Preferred	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
No leading zeros	2008: B7: 0:DEF0:DDDD: 0:E604: 1
Compressed	2008:B7::DEF0:DDDD:0:E604:1

Prefix length

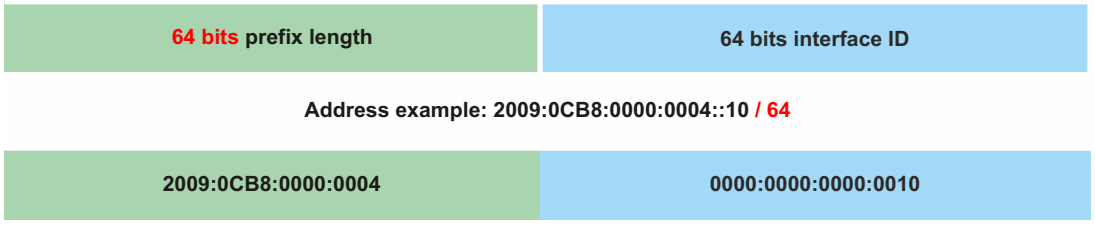
Unlike an IPv4 address, an IPv6 address does not use a subnet mask to identify the subnet part of the address. Instead, the IPv6 protocol uses the prefix length.

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.



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 9: IPv6 address types

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local Unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

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.

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.

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.

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 10: Link-Local Address format

10 bits	54 bits	64 bits
1111111010	0	Interface ID

The Link-Local address is specified and cannot be changed.

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.

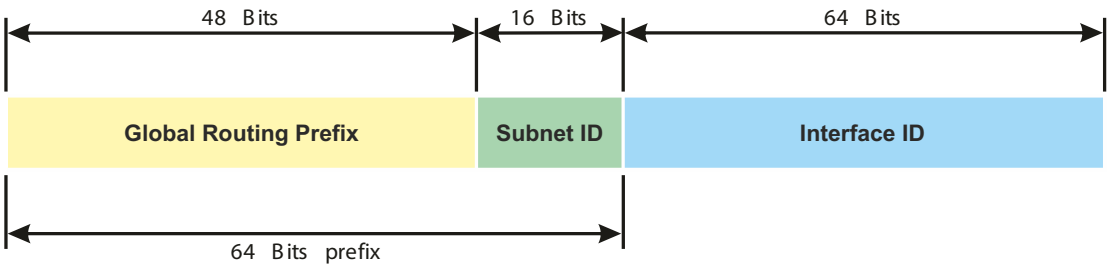


Figure 9: IPv6 Global Unicast address general format

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

The device lets you specify the IP parameters using the HiDiscovery protocol or using the Command Line Interface through the serial connection.

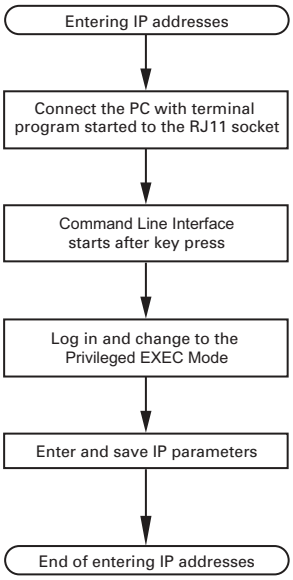
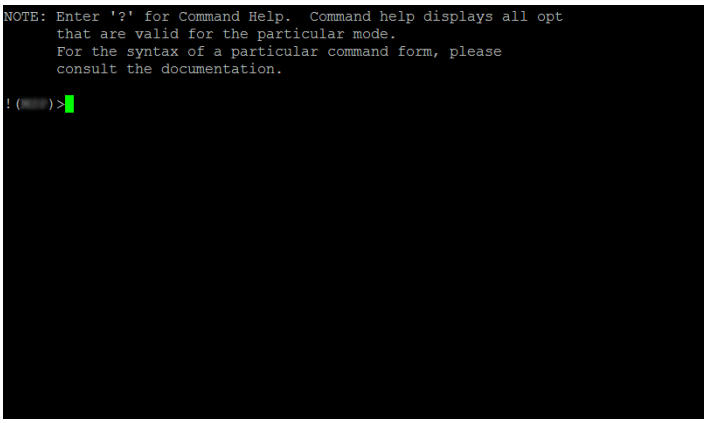


Figure 10: Flow chart for entering IP addresses

Note:
If a terminal or PC with terminal emulation is unavailable in the vicinity of the installation location, you can set up the device at your own workstation, then take it to its final installation location.

Perform the following steps:

- ☐ Set up a connection to the device.
  The start screen appears.



- ☐ Deactivate DHCP.
- ☐ Enter the IP parameters.
  - Local IP address
    In the default setting, the local IP address is `0.0.0.0`.
  - Netmask
    When you divided the network into subnets, 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 subnets (see on page 45 “How to use the netmask”).
    Specify the IP address of the gateway between the subnet 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`.

`enable`	To change to the Privileged EXEC mode.
`network protocol none`	To deactivate DHCP.
`network parms 10.0.1.23 255.255.255.0`	To assign the device the IP address `10.0.1.23` and the netmask `255.255.255.0`. You have the option of also assigning a *Gateway* address.
`copy config running-config nvm`	To save the current settings in the non-volatile memory (*NVM*) in the “Selected” configuration profile.

After entering the IP parameters, you easily set up the device using the Graphical User Interface.

2.2.2 IPv6

The device lets you specify the IPv6 parameters using the Command Line Interface through the serial connection. 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, an IPv6 address does not use a subnet mask to identify the subnet part of the address. This role is performed in IPv6 by the prefix length (see on page 49 “Prefix length”).
  - *EUI option* function
    You can use the *EUI option* function to automatically specify 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 `::`.

`enable`	To change to the Privileged EXEC mode.
`network ipv6 operation`	To enable the IPv6 protocol if the protocol is disabled. In the default setting, the IPv6 protocol is enabled.
`network ipv6 address add 2001::1 64 eui-64`	To assign the IPv6 address `2001::1` and the prefix length `64`. The `eui-64` parameter is optional. You have the option of also assigning a Gateway address.
`copy config running-config nvm`	To save the current settings in the non-volatile memory (*NVM*) in the “Selected” configuration profile.

After entering the IPv6 parameters, you easily set up 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 set up other parameters using the Graphical User Interface.

Perform the following steps:
- ☐ Install the HiDiscovery program on your computer.
- ☐ Start the HiDiscovery program.

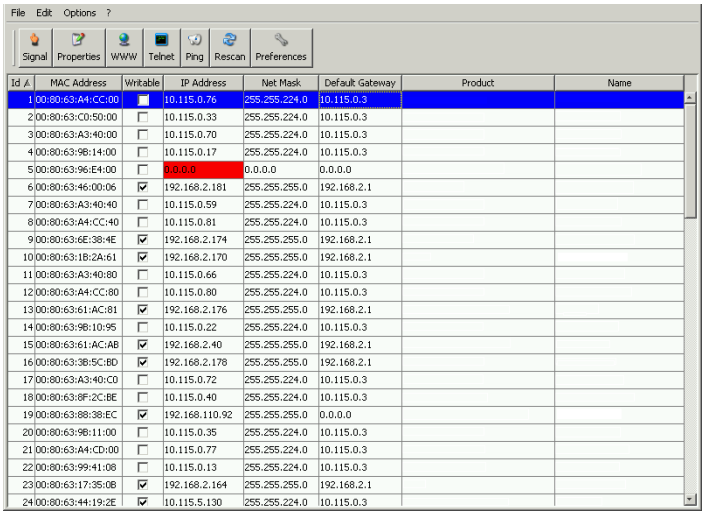


Figure 11: HiDiscovery

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 interfaces, you can select the desired network interface 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.

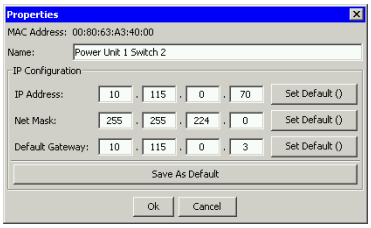


Figure 12: HiDiscovery – assigning IP parameters

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 set up 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.
- Apply 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 64 “Duplicate Address Detection function”).

Apply 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 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 specified 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 Dynamic Host Configuration Protocol (DHCP) 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 (*NVM*).

Table 11: DHCP options which the device requests

Options	Meaning
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Hostname
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

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. As an alternative, 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 assignment).

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 Dynamic Host Configuration Protocol (DHCP) for IPv4. DHCPv6 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 set up 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 specified release delay time.

When you disable active detection, the device sends 2 gratuitous ARP 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 specified 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

2.8 Duplicate Address Detection function

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 set up manually, or using the *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`)
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`network ipv6 dad-transmits <0..5>`	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 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 into the device management.
- ☐ Log into the device management with the default password.
  The device prompts you to type in a new 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 into the device management through the Command Line Interface, the device prompts you to confirm your new password.
- ☐ Log into the device management again with your new password.

Note:
If you lost your password, then contact your local support team.

3.2 Authentication lists

When a user accesses the device management using a specific connection, the device verifies the login credentials of the user through 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.

3.2.1 Applications

The device provides an application for each type of connection through which someone accesses the device:
- Access to the Command Line Interface using the 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`

3.2.2 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
- TACACS+

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)
- TACACS+

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.

3.2.3 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.

`show authlists`	To display the authentication lists that are set up.

☐ Deactivate the authentication list for those applications by means of which no access to the device is performed, for example `8021x`.

☐ In the *Active* column of the authentication list `defaultDot1x8021AuthList`, unmark the checkbox.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`authlists disable defaultDot1x8021AuthList`	To deactivate the authentication list `defaultDot1x8021AuthList`.

3.2.4 Adjusting 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 passes authentication requests to a RADIUS or TACACS+ 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.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`authlists add loginGUI`	To add the authentication list `loginGUI`.

☐ 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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

```
authlists set-policy  loginGUI radius local
reject reject reject
```

To assign the policies *radius*, *local* and *reject* to the authentication list loginGUI.

```
show authlists
```

To display the authentication lists that are set up.

☐ 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 dialog displays the updated settings:
- 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.

☐ Apply the settings temporarily. To do this, click the button.

```
show applists
```

To display the applications and the allocated lists.

```
applists set-authlist  WebInterface
loginGUI
```

To assign the loginGUI application to the authentication list WebInterface.

3.3 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 or TACACS+ 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.

3.3.1 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.

Note:
The following applies to the Command Line Interface: Users to whom a specific authorization profile is assigned are allowed to use commands and functions from this authorization profile or a lower level role. The commands available to a user also depend on the Command Line Interface mode in which the user is currently working. See “Mode-based command hierarchy” on page 23.

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.

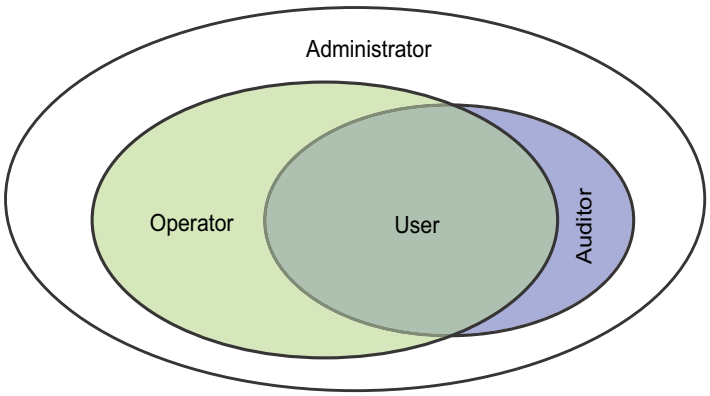


Figure 13: Access roles for user accounts

Table 12: Access roles for user accounts

Role	Description	Authorized for the following activities
administrator	The user is authorized to monitor and administer the device.	All activities with read/write access, including the following activities reserved for an administrator: • Add, modify or delete user accounts • Activate, deactivate or unlock user accounts • Change every password • Set up the password management • Set or change system time • Load files to the device, for example, device settings, certificates, or device software images • Reset settings and security-related settings to the state on delivery • Set up the RADIUS or TACACS+ server and the authentication lists • Apply scripts using the Command Line Interface • Enable/disable CLI logging and SNMP logging • External memory activation and deactivation • Activate or deactivate System Monitor 1 • Enable/disable the services for the access to the device management (for example SNMP). • Set up access restrictions to the Graphical User Interface or the Command Line Interface based on the IP addresses
operator	The user is authorized to monitor and set up the device, with the exception of security-related settings.	All activities with read/write access, with the exception of the above-named activities, which are reserved for an administrator:
auditor	The user is authorized to monitor the device and to save the log file in the *Diagnostics > Report > Audit Trail* dialog.	Monitoring activities with read access.
guest	The user is authorized to monitor the device - with the exception of security-related settings.	Monitoring activities with read access.
unauthorized	No access to the device possible. • As an administrator you assign this access role to temporarily lock a user account. • 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.	No activities allowed.

3.3.2 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.

`show users` — To display the user accounts that are set up.

3.3.3 Default user accounts

In the default setting, the user account `admin` is set up in the device.

Table 13: Settings of the default user account

Parameter	Default setting
User name	`admin`
Password	`private`
Role	*`administrator`*
User locked	`unmarked`
Policy check	`unmarked`
SNMP auth type	*`hmacmd5`*
SNMP encryption type	*`des`*

Change the password for the `admin` user account before making the device available in the network.

3.3.4 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 require a specified minimum complexity for the passwords, 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.

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 *Diagnostics > Status Configuration > Security Status* dialog.

- ☐ 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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users password-policy-check <user> enable`	To activate the checking of the password for the `<user>` user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.

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`.

`users password USER SECRET`	To specify the password `SECRET` for the user account `USER`. Enter at least 6 characters.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.3.5 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, you 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 set up the device, with the exception of security-related settings. To do this, perform the following steps:

☐ Create a user account.

- ☐ 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, you give the user account the name `USER`.
- ☐ Click the *Ok* button.
- ☐ To require a specified minimum complexity for the passwords, 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.

- ☐ 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.
- ☐ In the *Role* column, select the access role.
  In this example, you select the value *operator*.
- ☐ To activate the user account, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.
  The dialog displays the user accounts that are set up.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users add USER`	To add the `USER` user account.
`users password-policy-check USER enable`	To activate the checking of the password for the `USER` user account based on the specified policy. In this way, you require a specified minimum complexity for the passwords.
`users password USER SECRET`	To specify the password `SECRET` for the user account `USER`. Enter at least 6 characters.
`users access-role USER operator`	To assign the access role *operator* to the user account `USER`.
`users enable USER`	To activate the user account `USER`.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

Note:
When you are setting up a new user account in the Command Line Interface, remember to allocate the password.

3.3.6 Automatic unlocking of user accounts

When a user exceeds the maximum number of consecutive unsuccessful login attempts, the device locks the user account. If automatic unlocking of user accounts is enabled, the device unlocks locked user accounts automatically. Each account is unlocked after its specified wait time has elapsed. A user with the *administrator* access role can manually unlock a user account before the automatic unlock occurs.

Only a user with the *administrator* access role can enable/disable automatic user account unlocking and change the wait times. The wait time can be set individually for each user account.

Note:
A user cannot access the device management when the user account is locked. To help ensure continued access to the device management, the device does not lock the last user account with the *administrator* access role.

Enabling automatic unlocking of user accounts

The *Auto-unlock users* function is disabled by default. To enable the function, perform the following steps:

- ☐ Open the *Device Security > User Management* dialog.
  The dialog displays the user accounts that are set up on the device.
- ☐ Enable the *Auto-unlock users* function. To do this, in the *Configuration* frame, mark the *Auto-unlock users* checkbox.
- ☐ In the *Auto-unlock timer [min]* column of the relevant user account, specify the desired wait time.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`passwords auto-unlock-users`	To enable automatic unlocking of user accounts.
`user auto-unlock-timer USER1 40`	To specify a wait time of `40` minutes for the user account `USER1`. Specify the wait time as an integer. The user account name and wait time are examples only.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

Effect on locked user accounts

The device resets a running timer in the following cases:
- Disabling and re-enabling the *Auto-unlock users* function.
- Changing the wait time while the respective user account is locked and the timer is running.

In these cases, the device restarts the timer with the specified wait time. As a result, the account stays locked until the full wait time has elapsed.

Disabling automatic unlocking of user accounts

When automatic user account unlocking is disabled, any currently locked user accounts remain locked until a user with the *`administrator`* access role unlocks them. To disable automatic user account unlocking, perform the following steps:

- ☐ Open the *Device Security > User Management* dialog.
- ☐ Disable the *Auto-unlock users* function. To do this, in the *Configuration* frame, unmark the *Auto-unlock users* checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.

`configure`	To change to the Configuration mode.
`no passwords auto-unlock-users`	To disable automatic unlocking of user accounts.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.3.7 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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users disable <user>`	To disable user account.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

☐ To permanently deactivate the user account settings, you delete the user account.

- ☐ Select the table row of the relevant user account.
- ☐ Click the button.

`users delete <user>`	To delete the user account `<user>`.
`show users`	To display the user accounts that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.3.8 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 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 of consecutive unsuccessful 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 consecutive unsuccessful 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 unsuccessful 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 can attempt to log into the device management. 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.

☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`passwords min-length 6`	To specify the policy for the minimum length of the password.
`passwords min-lowercase-chars 1`	To specify the policy for the minimum number of lower-case letters in the password.
`passwords min-numeric-chars 1`	To specify the policy for the minimum number of digits in the password.
`passwords min-special-chars 1`	To specify the policy for the minimum number of special characters in the password.
`passwords min-uppercase-chars 1`	To specify the policy for the minimum number of upper-case letters in the password.
`show passwords`	To display the policies that are set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.4 LDAP function

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 transfer a digital certificate to the device. The certificate helps the device to verify the server for Secure Socket Layer (SSL) and Transport Layer Security (TLS) connections. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

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

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.

3.4.1 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 digital 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.

3.4.2 Setting up LDAP

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, you specify which attributes in the *Active Directory* contain the user login credentials and the permission level. The device then compares the user login credentials with the permission levels specified in the device and lets the user log into the device management at the assigned permission level.

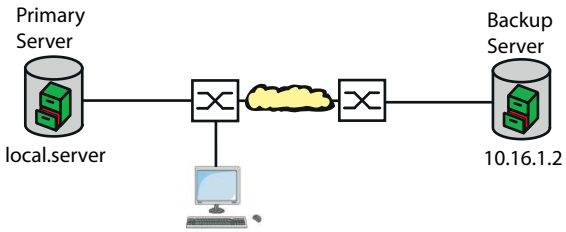


Figure 14: Application example of an LDAP setup

For this example, the server administrator sent the following information:

Information	Primary Server	Backup Server
The server name or IP address	`local.server`	`10.16.1.2`
The location of the *Active Directory* on the server	`Country/City/User`	`Country/Company/User`
The type of connection used	`TLS` (with digital certificate)	`SSL`
The server administrator sent the digital certificate in an email.	Digital certificate for primary server saved locally	Digital certificate for backup server saved locally
The TCP listening port	`389 (tls)`	`636 (ssl)`
Name of the attribute containing the user name	`userPrincipalName`	`userPrincipalName`
The names of the attribute containing the user permission levels	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Perform the following steps:

- ☐ Open the *Device Security > Authentication List* dialog.
- ☐ To set up the device to retrieve the user login credentials from the first *Active Directory*, 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 digital certificate to verify the identity of the server.

- ☐ When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- ☐ To transfer the file to 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 digital 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 Backup server administrator, add and activate another table row, then specify the settings in the corresponding columns.

- ☐ Open the *Device Security > LDAP > Role Mapping* dialog.
- ☐ To add a table row, click the button.

When a user logs into the device management, with LDAP set up 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 into the device management 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.
- ☐ Enable the *LDAP* function.
  Select the *`On`* radio button in the *Operation* frame.

The following table describes how to set up the *LDAP* function in the device using the Command Line Interface. The table displays the commands for *Index*=1. To set up other indexes, use the same commands and substitute the appropriate information.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ldap cache-timeout 1440`	To specify the device to flush the non-volatile memory after a day.
`ldap client server add 1 local.server port 389`	To add a connection to the remote authentication client server with the hostname `local.server` and the UDP port `389`.
`ldap client server modify 1 security startTLS`	To specify the type of security used for the connection.
`ldap client server modify 1 description Primary_AD_Server`	To specify the configuration name of the entry.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	To specify the Base Domain Name used to find the *Active Directory* on the server.
`ldap search-attr userPrincipalName`	To specify the attribute to search for in the *Active Directory* which contains the login credential of the users.
`ldap bind-user user@company.com`	To specify the name and domain of the service user.
`ldap bind-passwd Ur-123456`	To specify the password of the service user.
`ldap client server enable 1`	To enable the remote authentication client server connection.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	To add a remote authentication role mapping entry for the access role *`operator`*. Map the access role *`operator`* to the attribute containing the word `OPERATOR`.
`ldap mapping enable 1`	To enable the remote authentication role mapping entry.
`ldap operation`	To enable the remote authentication function.

3.5 SNMP access

The Simple Network Management Protocol (SNMP) lets you work with a network management system to monitor the device over the network and change its settings.

3.5.1 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-only* access and `private` for *read and write* access 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 and write* access than for *read-only* access.
- ☐ Use SNMPv1 or SNMPv2 only in environments protected from eavesdropping. The protocols do not use encryption.
- ☐ Deactivate the write access for the SNMPv1/v2 `Write` community.
- ☐ We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

3.5.2 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 the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users snmpv3 authentication <user> <auth type>`	To specify the algorithm that the device uses to authenticate the SNMPv3 user `<user>`. Possible `<auth type>` values: • `md5` • `sha1` • `sha256`
`users snmpv3 encryption <user> <encryption type>`	To specify the algorithm that the device uses to encrypt SNMPv3 messages for the SNMPv3 user `<user>`. Possible `<encryption type>` values: • `des` • `aescfb128` • `aescfb256` • `none` (no encryption)
`show users`	To display the user accounts that have been set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.5.3 SNMPv3 traps

SNMP version 3 lets the device use encrypted communication with a network management system.

For this, you need to set up the following roles in the device:
- SNMPv3 trap users
- SNMPv3 trap hosts

SNMPv3 trap users

An SNMPv3 trap user has the permission to send SNMPv3 traps to the specified SNMPv3 trap hosts.

An SNMPv3 trap user is exclusively for sending SNMPv3 traps to SNMPv3 trap hosts. Do not confuse SNMPv3 trap users with device user accounts. See section “Managing user accounts” on page 71.

The device supports encryption and authentication for sending SNMPv3 traps. The device lets you set up a maximum of 10 SNMPv3 trap users.

The device supports the following authentication and encryption types:

- `auth-no-priv`
  The user needs to authenticate to send SNMPv3 traps. The device sends the SNMPv3 traps unencrypted.
- `auth-priv`
  The user needs to authenticate to send SNMPv3 traps. The device sends the SNMPv3 traps encrypted.
- `no-auth`
  Do not use this setting if you transmit data over untrusted networks.
  The device sends the SNMPv3 traps unencrypted without authentication.

To add an SNMPv3 trap user, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification user add <name1> auth-priv auth <authentication algorithm> <passphrase1> priv <encryption algorithm> <passphrase2>`	To add the SNMPv3 trap user `<name1>` with authentication and encryption: • `<authentication algorithm>` Possible values: – `md5` – `sha1` – `sha256` (recommended) • `<passphrase1>` authentication passphrase • `<encryption algorithm>` Possible values: – `des` – `aescfb128` – `aescfb256` (recommended) • `<passphrase2>` encryption passphrase
`show snmp notification users`	To display the SNMPv3 trap user settings.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

To modify an existing SNMPv3 trap user, delete the user and add a new user with the desired settings.

To delete an SNMPv3 trap user, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification user delete <name1>`	To delete the SNMPv3 trap user `<name1>`.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

SNMPv3 trap hosts

An SNMPv3 trap host is the destination for an SNMPv3 trap that the device sends.

The device supports a maximum of 10 SNMPv3 trap hosts.

To specify an SNMPv3 trap host, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification host add <hostname1> a.b.c.d user <name2> auth-priv`	To add the SNMPv3 trap host `<hostname1>` • With the IPv4 address `<a.b.c.d>` • Username `<name2>` • With authentication and encryption
`show snmp notification hosts`	To display the SNMPv3 trap host settings.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

To modify an existing SNMPv3 trap host, delete the host and add a new host with the desired settings.

To delete an SNMPv3 trap host, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp notification host delete <hostname1>`	To delete the SNMPv3 trap host `<hostname1>`.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.6 Out-of-Band access

The device has 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.

In the default setting, you can access the device management through this port using the following IP parameters:
- *IP address* 192.168.1.1
- *Netmask* 255.255.255.0

To access the device management, assign an IP address in the same subnet to the management station.

The device lets you access the device management using the following protocols:
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.6.1 Specifying the IP parameters

In the default setting, the *Service Port* has static IP parameters. The device lets you change the IP parameters to adapt the device to the requirements of your environment. You can also use an external DHCP server to specify the IP parameters for the *Service Port* network interface.

Verify that the IP subnet of this network interface does not overlap with any subnet connected to another interface of the device:
- Management interface

If the management station accesses the device management through the *Service Port*, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Specifying static IP parameters

Perform the following steps:

- ☐ Open the *Basic Settings > Out-of-Band* dialog.
- ☐ Overwrite the IP address in the *IP parameter* frame, *IP address* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
network out-of-band parms 192.168.1.1
255.255.255.0 192.168.1.254
```
To specify the IP address `192.168.1.1` and the netmask `255.255.255.0` for the *Service Port* network interface, and the IP address `192.168.1.254` for the *default gateway*.

```
show network out-of-band
```
To display the *Service Port* network interface settings.

```
Out-of-band management settings
------------------------------
Management operation.....................enabled
Interface status.........................up
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Default gateway address..................192.168.1.254
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................none
```

```
save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

Specifying the IP parameters using a DCHP server

Perform the following steps:

- ☐ Open the *Basic Settings > Out-of-Band* dialog.
- ☐ In the *Management interface* frame, select the *DHCP* radio button in the *IP address assignment* option list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
network out-of-band protocol dhcp
```
To select `dhcp` as the *Service Port* configuration protocol.

```
show network out-of-band
```
To display the *Service Port* network interface settings.

```
Out-of-band management settings
------------------------------
Management operation.....................enabled
Interface status.........................up
IP address...............................0.0.0.0
Subnet mask..............................0.0.0.0
Default gateway address..................0.0.0.0
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................dhcp
```

```
save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.6.2 Disabling the Service Port network interface

In the default setting, the *Service Port* network interface is enabled. If you do not want someone to access device management through the *Service Port* port, then the device lets you disable the *Service Port* network interface.

If the management station accesses the device management through the *Service Port*, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you perform the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out-of-Band* dialog.
- ☐ Disable the *Service Port* network interface.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

```
enable
```
To change to the Privileged EXEC mode.

```
no network out-of-band operation
```
To disable the *Service Port* network interface.

```
Out-of-band management settings
------------------------------
Management operation.....................disabled
Interface status.........................down
IP address...............................0.0.0.0
Subnet mask..............................0.0.0.0
Default gateway address..................0.0.0.0
MAC address..............................ec:e5:55:f6:f7:a9
Configuration protocol...................dhcp

save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.7 TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol used for centralized user authentication and authorization. The TACACS+ protocol helps verify the identity of a user who is trying to access a network device. It also supports fine-grained control over which Command Line Interface commands the user is permitted to execute on the device.

Compared to the RADIUS protocol, the TACACS+ protocol helps ensure higher security by obfuscating the entire communication.

The prerequisite for using TACACS+ on the device is that a TACACS+ server is available in the network.

The TACACS+ protocol controls access to the device over the following connections:
- Telnet
- SSH
- Serial connection

The TACACS+ protocol has the following benefits for administrators:
- General control over the access role to be assigned to an authenticated user.
- Fine-grained control over the Command Line Interface commands that the user is allowed to execute.
- Tracking actions performed by authenticated users on the device.

3.7.1 Setting up a TACACS+ server entry on the device

To use TACACS+ on the device, set up at least one TACACS+ server entry. TACACS+ uses the TCP port 49 for communication between the client and the server. You can specify a different port on the device, if necessary.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server add {<ipv4> | <ipv6> | <dns name>}`	To specify the TACACS+ server address.
`tacacs server modify {<ipv4> | <ipv6> | <dns name>} port <port>`	To modify the TCP port through which the device communicates with the TACACS+ server.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

3.7.2 Specifying the parameters of an individual TACACS+ server entry

For obfuscated communication between the device and a TACACS+ server, you can specify an individual TACACS+ server key.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server modify {<ipv4> | <ipv6> | <dns name>} key`	To specify a TACACS+ server key that the device uses for the communication with this specific TACACS+ server. Press the <Enter> key.
`Enter key (128 characters max): <key>`	Enter the new key. The maximum length of the key is 128 ASCII characters. Enter a key that contains at least 16 characters. Press the <Enter> key.
`Re-enter key: <key>`	Re-enter the new key. Press the <Enter> key.
`Key has been changed!`	The individual TACACS+ server key is changed.
`tacacs server modify timeout 1`	To specify the value of `1` second as the timeout period that the device waits until the TACACS+ server responds. Values in the range `1`..`30` are allowed.
`tacacs server modify priority 0`	To change the priority of the TACACS+ server to `0`, the highest priority. Values in the range `0`..`65535` are allowed.
`tacacs server modify {<ipv4> | <ipv6> | <dns name>}`	To change the TACACS+ server address. If the TACACS+ server is using an IPv6 link-local address, then specify the value `link-local-intf cpu/1`.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

3.7.3 Specifying the global parameters for every TACACS+ server entry

For obfuscated communication between the device and multiple TACACS+ servers, you can specify global parameters, for example a global TACACS+ server key. The device will use this key if no key is specified for an individual TACACS+ server entry.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs server key`	To specify a TACACS+ server key that the device can use for the communication with multiple TACACS+ servers. Press the <Enter> key.
`Enter key (128 characters max): <key>`	Enter the new key. The maximum length of the key is 128 ASCII characters. Enter a key that contains at least 16 characters. Press the <Enter> key.

`Re-enter key: <key>`	Re-enter the new key. Press the <Enter> key.
`Key has been changed!`	The global TACACS+ server key is changed.
`tacacs server timeout 1`	To specify the value of `1` second as the timeout period that the device waits until the TACACS+ server responds. Values in the range `1..30` are allowed.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

3.7.4 Authenticating users through TACACS+

To authenticate users through a TACACS+ server, add the `tacacs` policy to an authentication list. See section “Authentication lists” on page 66.

The device provides you with the following options:
- Adding the `tacacs` policy to an existing authentication list.
- Creating a new authentication list and adding the `tacacs` policy to this authentication list.

During authentication, the TACACS+ server assigns a privilege level to the user, which determines the corresponding access role on the device. Depending on the allocated access role, the user has access to a specific set of commands. This set of commands is preset on the device for each access role. See section “Access roles” on page 69.

In the following example, you set up `tacacs` as the first policy the device uses to authenticate users who log on to the device over the serial connection.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`authlists set-policy defaultV24AuthList tacacs local radius reject reject`	To specify `tacacs` as the first policy of the preset authentication list `defaultV24AuthList`.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

3.7.5 Authorizing commands through TACACS+

If command authorization is disabled, then the user has access to the entire set of commands preset for the access role assigned during authentication. This set of commands is preset on the device for each access role. See section “Access roles” on page 69.

If command authorization is enabled, then the device checks with the TACACS+ server each command that the user wants to execute on the device. The TACACS+ server then determines whether the user is allowed to execute the respective command.

For already logged-in users, the status of command authorization remains unchanged. Any changes to the status of command authorization take effect only after the user logs out and in again.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs cmd-authorization operation`	To enable command authorization.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

3.7.6 Accounting user activity on the device

The accounting function of the TACACS+ protocol tracks actions performed by authenticated users on the device. The device generates a record for every successful user action. The device immediately sends each generated record to the TACACS+ server in the network. This helps the network administrator or security officers get an overview of the successful user actions performed on network devices.

The device supports the *stop-only* mode of the TACACS+ accounting function. The device tracks user activity, even if the user authenticated through a protocol other than TACACS+.

When you enable the accounting function, the device generates one of the following records when a relevant event occurs:
- *Login record*
  when a user session starts
- *Accounting record*
  for each command successfully executed during a user session
- *Logout record*
  when a user session ends

Security considerations:
- The TACACS+ accounting function does not record unsuccessful login attempts nor attempts to execute disallowed commands.
- The information exchanged between the device and the TACACS+ server is only obfuscated by the TACACS+ protocol, not encrypted. Use the TACACS+ accounting function only if you can accept this level of security.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`tacacs accounting command mode stop-only`	To enable accounting on the device.
`show tacacs global`	To display the status of the accounting function.
`TACACS+ client global settings`	
`----------`	
`...`	
`TACACS+ command accounting mode.....stop-only`	
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Privileged EXEC mode.

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 in the network using the following options:
- The Simple Network Time Protocol (SNTP) is a simple solution for low accuracy requirements. Under ideal conditions, the Simple Network Time Protocol (SNTP) achieves accuracy in the millisecond range. The accuracy depends on the signal delay.
- The Precision Time Protocol (PTP) along with IEEE 1588 achieves accuracy on the order of sub-microseconds. This protocol is suitable for demanding applications up to and including process control.

When the involved devices support the Precision Time Protocol (PTP), it is the better choice. The Precision Time Protocol (PTP) is more accurate, has advanced methods of error correction, and causes only a low network load. The implementation of the Precision Time Protocol (PTP) is comparatively easy.

Note:
According to the Precision Time Protocol (PTP) and Simple Network Time Protocol (SNTP) standards, both protocols can operate in parallel in the same network. However, since both protocols can influence the system time of the device, situations can occur in which the two protocols conflict with each other.

4.1 Setting the time

When there is no reference time source available to you, you can manually set the system time in the device.

When you start the device after it has been powered down for some time, it initializes the clock with January 1 2026, 01:00 UTC+1. After powered down, the device buffers the settings of its real-time clock for up to 24 hours.

As an alternative, you can set up the device to obtain the current time using one of the following protocols:
- Simple Network Time Protocol
- Precision Time Protocol

Perform the following steps:

☐ Open the *Time > Basic Settings* dialog.

- The *System time (UTC)* field displays the date and time of the device system clock with reference to Universal Time Coordinated (UTC). 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.

Note:
PTP sends the International Atomic Time (TAI). As of July 1, 2020, the TAI time is 37 s ahead of the Universal Time Coordinated (UTC). When the PTP reference time source of the UTC offset is set correctly, the device automatically corrects this difference on the display in the *System time (UTC)* field.

☐ To make the device apply the time of your computer 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`.
  When PTP is active and the device receives a valid PTP message, the device sets its time source to `ptp`. The device prioritizes PTP ahead of SNTP.
- The *Local offset [min]* value specifies the difference in minutes between Universal Time Coordinated (UTC) and local time.

☐ To cause the device to determine the time zone on your PC, click the *Set time from PC* button. The device calculates the difference between local time and Universal Time Coordinated (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.

☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	To set the system time of the device.
`clock timezone offset <-780..840>`	To enter the difference in minutes between the local time and the received Universal Time Coordinated (UTC).
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

4.2 Automatic daylight saving time changeover

When you operate the device in a time zone with a summer time change, the device lets you set up the automatic daylight saving time changeover.

If the *Daylight saving time* mode is enabled, the device advances the local system time by one hour during the summer time. At the end of summer time, the device sets the local system time back again by one hour.

4.2.1 Setting daylight saving time using pre-defined profiles

The device lets you specify the start and end of daylight saving time using pre-defined profiles.

The device includes the following pre-defined profiles:

- *EU*
  Daylight saving time settings as applicable in the European Union.
- *USA*
  Daylight saving time settings as applicable in the United States of America.

To select the *EU* profile for the daylight saving time settings, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ In the *Operation* frame, click the *Profile...* button.
- ☐ Select the *EU* item from the *Profile...* list.
  Selecting a profile overwrites the settings specified in the *Summertime begin* and *Summertime end* frames.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode eu`	To enable the *Daylight saving time* mode with the profile `eu`.

4.2.2 Setting daylight saving time manually

The network administrator wants to specify the following daylight saving time settings:

Summertime begin
- *Week* = `Last`
- *Day* = `Sunday`
- *Month* = `March`
- *System time* = `02:00`

Summertime end
- *Week* = `Last`
- *Day* = `Sunday`

- *Month* = *October*
- *System time* = 03:00

For the purpose described above, perform the following steps:

- ☐ Open the *Time > Basic Settings* dialog, *Daylight saving time* tab.
- ☐ Enable the *Daylight saving time* mode.
  Select the *On* radio button in the *Operation* frame.
- ☐ In the *Summertime begin* frame, specify the following settings:
  - *Week* = *Last*
  - *Day* = *Sunday*
  - *Month* = *March*
  - *System time* = 02:00
- ☐ In the *Summertime end* frame, specify the following settings:
  - *Week* = *Last*
  - *Day* = *Sunday*
  - *Month* = *October*
  - *System time* = 03:00
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`clock summer-time mode recurring`	To enable the *Daylight saving time* mode.
`clock summer-time recurring start last sun mar 02:00`	To specify the time at which the device sets the clock forward from standard time to summer time. • `last` To specify the *Last* week in the month. • `sun` To specify the day *Sunday*. • `mar` To specify the month *March*. • `02:00` To specify the time 02:00.
`clock summer-time recurring end last sun oct 03:00`	To specify the time at which the device resets the clock from summer time to standard time. • `last` To specify the *Last* week in the month. • `sun` To specify the day *Sunday*. • `oct` To specify the month *October*. • `03:00` To specify the time 03:00.

4.3 Synchronizing time in the network with SNTP

The Simple Network Time Protocol (SNTP) lets you synchronize the system time in the network. The device supports the SNTP client and the SNTP server function.

The SNTP server makes the Universal Time Coordinated (UTC) available. 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.

SNTP is a simplified version of Network Time Protocol (NTP). 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 14: Target IPv4 address classes for Broadcast operation mode

IPv4 destination address	Send SNTP packets to
`0.0.0.0`	Nobody
`224.0.1.1`	*Multicast* address for SNTP messages
`255.255.255.255`	*Broadcast* address

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.

4.3.1 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.

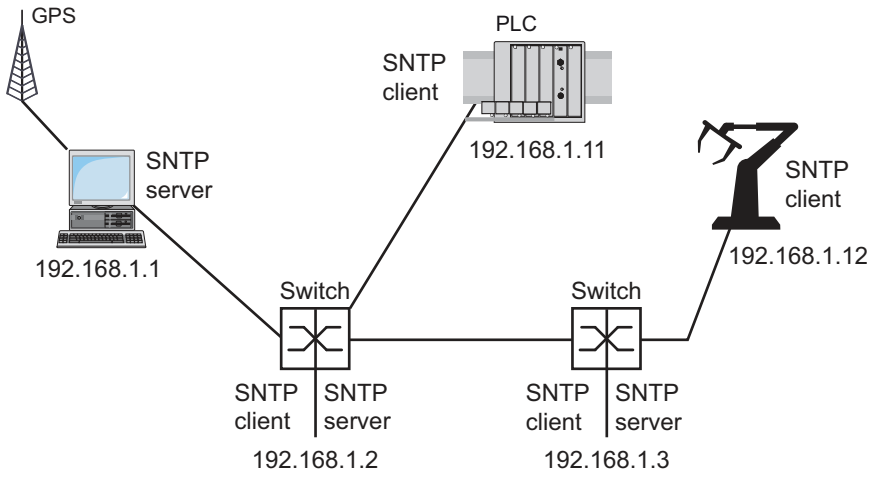


Figure 15: Example of SNTP cascade

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 set-up SNTP servers. When there is no response from the first SNTP server, the SNTP client sends its requests to the second SNTP server. When this request is also unsuccessful, it sends the request to the 3rd and finally to 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.

4.3.2 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.
- ☐ Specify the connection data of the SNTP server.
- ☐ Enable the *Client* function.
  Select the `On` radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- The *State* field displays the current status of the *Client* function.

Table 15: SNTP client settings for the example

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Client function	`Off`	`On`	`On`	`On`	`On`
Configuration: *Mode*	`unicast`	`unicast`	`unicast`	`unicast`	`unicast`
Request interval [s]	`30`	`30`	`30`	`30`	`30`

Server address(es)	–	`192.168.1.1`	`192.168.1.21`
			`92.168.1.1`
				`192.168.1.21`
				`92.168.1.1`
					`192.168.1.31`
					`92.168.1.219`
					`2.168.1.1`

4.3.3 Specifying SNTP server settings

When operating as an SNTP server, the device distributes its system time as Universal Time Coordinated (UTC) to the network. To do this, perform the following steps:

- Open the *Time > SNTP > Server* dialog.
- Enable the *Server* function.
  Select the *On* radio button in the *Operation* frame.
- 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 IPv6 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 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.
- Apply the settings temporarily. To do this, click the button.
- The *State* field displays the current status of the *Server* function.

Table 16: Settings for the example

Device	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Server function	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	unmarked	unmarked	unmarked	unmarked	unmarked
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	unmarked	unmarked	unmarked	unmarked	unmarked

4.4 Synchronizing time in the network with PTP

For LAN-controlled applications to operate without latency, precise time management is required. With Precision Time Protocol (PTP), IEEE 1588 describes a method that enables precise synchronization of clocks in the network.

The *PTP* function in the device permits time synchronization with an accuracy of a few 100 ns. The *PTP* function uses Multicasts for the synchronization messages, therefore keeping the network load low.

4.4.1 Types of clocks

PTP defines the roles of “master” and “slave” for the clocks in the network:
- A master clock (reference time source) distributes its time.
- A slave clock synchronizes itself with the timing signal received from the master clock.

Boundary clock

The transmission time (latency) in routers and switches has a measurable effect on the precision of the time transmission. To correct such inaccuracies, PTP defines what are known as boundary clocks.

In a network segment, a boundary clock is the reference time source (master clock) to which the subordinate slave clocks synchronize. Typically routers and switches take on the role of boundary clock.

The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).

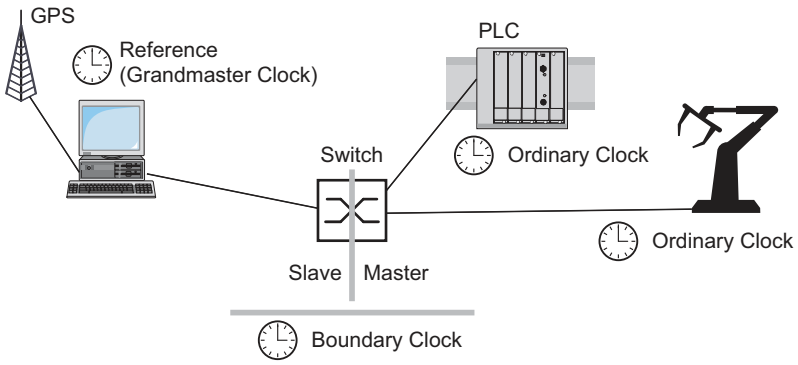


Figure 16: Position of the boundary clock in a network

Transparent Clock

Switches typically take on the *Transparent Clock* role to enable high accuracy across the cascades. The *Transparent Clock* is a *Slave* clock that corrects its own transmission time when it forwards received synchronization messages.

Ordinary Clock

PTP designates the clock in a end device as an *Ordinary Clock*. An *Ordinary Clock* functions either as a master clock or slave clock.

4.4.2 Best Master Clock algorithm

The devices participating in PTP designate a device in the network as a reference time source (Grandmaster). Here the *Best Master Clock* algorithm is used, which determines the accuracy of the clocks available in the network.

The *Best Master Clock* algorithm evaluates the following criteria:
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

The algorithm first evaluates the value in the *Priority 1* field of the participating devices. The device with the numerically lowest value in the *Priority 1* field is designated as the reference time source (*Grandmaster*). If the value is the same for multiple devices, then the algorithm takes the next criterion. If this is also the same, then the algorithm takes the next criterion after this one. If these values are the same for multiple devices, then the numerically lowest value in the *Clock identity* field decides which device is designated as the reference time source (*Grandmaster*). The value in the *Clock identity* field is based on the device MAC address which is supposed to be globally unique. The value in the *Clock identity* field serves as the final tie-break for the algorithm.

In the settings of the boundary clock, the device lets you individually specify the values for *Priority 1* and *Priority 2*. This lets you influence which device will be the reference time source (*Grandmaster*) in the network.

4.4.3 Delay measurement

The delay of the synchronization messages between the devices affects the accuracy. The delay measurement lets the devices take into account the average delay.

PTP version 2 offers the following methods for delay measurement:
- `e2e` (End to End)
  The slave clock measures the delay of synchronization messages to the master clock.
- `e2e-optimized`
  The slave clock measures the delay of synchronization messages to the master clock.
  This method is available only for transparent clocks. The device forwards the synchronization messages sent using Multicast only to the master clock, keeping the network load low. When the device receives a synchronization message from another master clock, it forwards the synchronization messages only to this new port.
  When the device knows no master clock, it forwards synchronization messages to every port.
- `p2p` (Peer to Peer)
  The slave clock measures the delay of synchronization messages to the master clock.
  In addition, the master clock measures the delay to each slave clock, even across blocked ports. This requires that the master and slave clock support Peer-to-Peer (`p2p`).
  In case of interruption of a redundant ring, for example, the slave clock becomes the master clock and the master clock becomes the slave clock. This switch occurs without loss of precision, because the clocks already know the delay in the other direction.

4.4.4 PTP domains

The device transmits synchronization messages only from and to devices in the same PTP domain. The device lets you set the domain for the boundary clock and for the transparent clock individually.

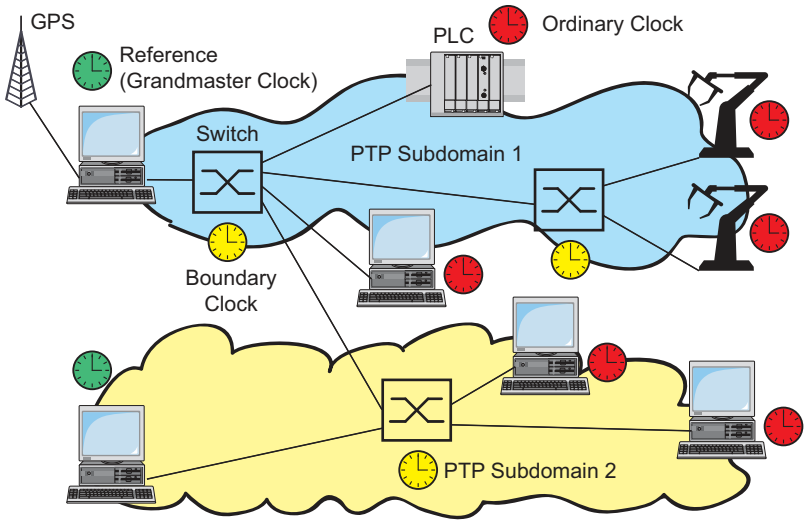


Figure 17: Example of PTP domains

4.4.5 Using PTP

To synchronize the clocks precisely with PTP, only use switches with a boundary clock or transparent clock as nodes.

Perform the following steps:

- ☐ To gain an overview of the distribution of clocks, draw a network plan with the devices involved in PTP.
- ☐ Specify the role for each participating switch (boundary clock or transparent clock). In the device, this setting is called *PTP mode*.

Table 17: Possible settings for PTP mode

PTP mode	Application
`v2-boundary-clock`	As a boundary clock, the device distributes synchronization messages to the slave clocks in the subordinate network segment. The boundary clock in turn obtains the time from a higher-level reference time source (Grandmaster).
`v2-transparent-clock`	As a transparent clock, the device forwards received synchronization messages after they have been corrected by the delay of the transparent clock.

- ☐ Enable PTP on each participating switch.
  PTP then sets itself up on a largely automatic basis.
- ☐ Enable PTP on the end devices.
- ☐ The device lets you influence which device in the network becomes the reference clock (Grandmaster). Therefore, change the default value in the *Priority 1* and *Priority 2* fields for the *Boundary Clock*.

4.4.6 Selecting the ports used for PTP

You have the option to select the ports that the device uses for synchronizing time with PTP:
- `internal`
- `external`

The default setting is `internal`.

For further information about the `internal` and `external` ports, see the “Installation” user manual.

The newly selected ports can be used for setting up PTP only after saving the configuration and rebooting the device.

In this example, you select the `external` ports for synchronizing time with PTP. To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ptp select-ports external`	To select the external ports for time synchronization with PTP.
`The change will take effect after saving the configuration and rebooting the device.` `Are you sure (Y/N)?`	Press the <Y> key.
`show ptp global`	To check the selected ports for PTP (`PTP Selected Ports`) and the ports currently used for PTP (`PTP Active Ports`).

`PTP Status`
`----------`
`...`
`PTP Selected Ports.....external`
`PTP Active Ports.....internal`
`...`	

`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

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.

To keep the changes after a reboot, the device lets you save the settings in a configuration profile in the non-volatile memory (*NVM*). To make it possible to quickly switch to other settings, the non-volatile memory (*NVM*) offers storage space for multiple configuration profiles.

If an external memory (*ENVM*) 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 (*NVM*) 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 (*ENVM*) and non-volatile memory (*NVM*)

You can recognize if the settings copied to the external memory (*ENVM*) 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). 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.

`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

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 the device adds a configuration profile in the non-volatile memory (*NVM*) or overwrites 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`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config running-config nvm profile <string>`	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”.

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`.

`enable`	To change to the Privileged EXEC mode.
`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`configure`	To change to the Configuration mode.
`config profile select nvm 1`	To select the configuration profile. Take note of the adjacent name of the configuration profile.
`save`	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 (*ENVM*)

When an external memory (*ENVM*) 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 to enable the device to automatically save a copy in the external memory (*ENVM*) during the saving process.
- ☐ To deactivate the function, unmark the checkbox in the *Backup config when saving* column.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm config-save sd` `config envm config-save usb`	To enable the function. When you save a configuration profile, the device saves a copy in the external memory (*ENVM*). *sd* = External SD memory *usb* = External USB memory
`no config envm config-save sd` `no config envm config-save usb`	To disable the function. The device does not save a copy in the external memory (*ENVM*). *sd* = External SD memory *usb* = External USB memory
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

5.2.3 Backing up the configuration profile on a remote server

The device lets you automatically back up 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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`show config remote-backup`	To check the status of the function.
`configure`	To change to the Configuration mode.
`config remote-backup destination {URL}`	To enter the destination URL for the configuration profile backup (max. 128 chars).
`config remote-backup username {username}`	To enter the user name to authenticate on the remote server (max. 128 chars).
`config remote-backup password {password}`	To enter the password to authenticate on the remote server (max. 128 chars).
`config remote-backup operation`	To enable the function.

If the transfer to the remote server is unsuccessful, then the device logs this event in the 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 server available 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.
- Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

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 for the file in the following form:
    `ftp://<user>:<password>@<IP address>[:port]/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ To save the file on a TFTP server, specify the URL for the file in the following form:
    `tftp://<IP address>/<path>/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ 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://<user>:<password>@<IP address>/<path>/<file name>`
    `scp://` or `sftp://<IP address>/<path>/<file name>`
    Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog. When you click the *Ok* button, the device displays the *Credentials* window. There you enter *User name* and *Password* to log into the server.
- ☐ Click the *Ok* button.
  The configuration profile is now saved as an XML file in the specified location.

`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	To save the current settings on a TFTP server. Do not use this method if you transmit data over untrusted networks.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	To save the “Selected” configuration profile in the non-volatile memory (`nvm`) on a SFTP server.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	To save the configuration profile `config3` in the non-volatile memory (`nvm`) on a TFTP server. Do not use this method if you transmit data over untrusted networks.
`copy config nvm profile config3 remote ftp://<IP_address>[:port]/<path>/<file_name>`	To save the configuration profile `config3` in the non-volatile memory (`nvm`) on an FTP server. Do not use this method if you transmit data over untrusted networks.

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`	To display the configuration profiles contained in the non-volatile memory (nvm).
`enable`	To change to the Privileged EXEC mode.
`copy config nvm profile config3 running-config`	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 (*ENVM*)

If an external memory (*ENVM*) is connected, then the device loads a configuration profile from the external memory (*ENVM*) during the system startup automatically. The device lets you save these settings in a configuration profile in non-volatile memory (*NVM*).

When the external memory (*ENVM*) 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 (*ENVM*) 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*.

☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`config envm load-priority sd first`	To enable the function. During the system startup, the device loads a configuration profile from the external memory (*ENVM*). *sd* = External SD memory
`config envm load-priority usb first`	To enable the function. During the system startup, the device loads a configuration profile from the external memory (*ENVM*). *usb* = External USB memory
`show config envm settings`	To display the settings of the external memory (*ENVM*).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
sd     ok          [x]         [x]         second
usb    ok          [x]         [x]         first
```

`save`	To save the settings in a configuration profile in the non-volatile memory (*NVM*) of the device.

Using the Command Line Interface, the device lets you copy the settings from the external memory (*ENVM*) directly into the non-volatile memory (*NVM*).

`show config profiles nvm`	To display the configuration profiles contained in the non-volatile memory (`nvm`).
`enable`	To change to the Privileged EXEC mode.
`copy config envm profile config3 nvm`	To copy the configuration profile `config3` from the external memory (*ENVM*) to the non-volatile memory (*NVM*).

The device can also automatically load a configuration profile from a script file during the system startup.

Prerequisites:
- Verify that the external memory (*ENVM*) is connected before you start the device.
- The root directory of the external memory (*ENVM*) 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 (*ENVM*) 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 (*ENVM*) 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 (*ENVM*). When you type the appropriate command into the script file, you have the option to disable this function:

☐ `no config envm config-save sd`
The device does not save a copy in the external SD memory.

☐ `no config envm config-save usb`
The device does not save 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 System Log.

5.3.3 Importing a configuration profile

The device lets you import a configuration profile saved as an XML file from a server. If you use the Graphical User Interface, then you can import the XML file directly from your PC.

Prerequisites:
- To import a file from a server, you need a server available on the network.
- To import a file through SCP or SFTP, you also need the user name and password for accessing this server.
- Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.

Perform the following steps:

☐ Open the *Basic Settings > Load/Save* dialog.

☐ Click the ☰ button and then the *Import...* item.
The dialog displays the *Import...* window.

☐ 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 selected external memory (*ENVM*).

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 your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
  - ☐ If the file is on an FTP server, then specify the URL in the following form:
    `ftp://<user>:<password>@<IP address>[:port]/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ If the file is on a TFTP server, then specify the URL in the following form:
    `tftp://<IP address>/<path>/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
    `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 into the server.
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.
- ☐ 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* 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 `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 (*ENVM*). 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 (*ENVM*) 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 `ram` in the *Destination* frame, then the device disconnects the Graphical User Interface and uses the settings immediately.

`enable`	To change to the Privileged EXEC mode.
`copy config remote ftp://<IP_address>[:port]/<path>/<file_name> running-config`	To import and activate the settings of a configuration profile saved on an FTP server. Do not use this method if you transmit data over untrusted networks. 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> running-config`	To import and activate the settings of a configuration profile saved on a TFTP server. Do not use this method if you transmit data over untrusted networks. 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> nvm profile config3`	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`). Do not use this method if you transmit data over untrusted networks.
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	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`). Do not use this method if you transmit data over untrusted networks.

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

5.4 Resetting the device to the default setting

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 (*ENVM*) is connected, then the device also deletes the configuration profiles saved in the external memory (*ENVM*).

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 (*ENVM*) is connected, then the device also deletes the configuration profiles saved in the external memory (*ENVM*).

After a brief period, the device restarts and loads the delivery settings.

`enable`	To change to the Privileged EXEC mode.
`clear factory`	To delete the configuration profiles from the non-volatile memory (*NVM*) and from the external memory (*ENVM*). If an external memory (*ENVM*) is connected, then the device also deletes the configuration profiles saved in the external memory (*ENVM*). After a brief period, the device restarts and loads the delivery settings.

5.4.2 Using System Monitor 1

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 System Monitor 1, press the <1> key within 3 seconds when prompted during reboot.
  The device displays System Monitor 1.
- ☐ 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 (*ENVM*) is connected, then the device also deletes the configuration profiles saved in the external memory (*ENVM*).
- ☐ To change to the main menu, press the <q> key.
- ☐ To reboot the device with factory settings, press the <q> key.

6 Updating the device software

Hirschmann is continually working on improving and developing their software. Check regularly if there is an updated version of the device software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at catalog.belden.com.

The device gives you the following options to update the device software:
- Loading a previous device software version
- Software update from the PC
- Software update from a server
- Software update from the external memory (ENVM)

Note:
The device settings are kept after you update 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 device software when you are already logged into the device management, perform the following steps:

☐ Open the *Basic Settings > Software* dialog.
The *Running version* field displays the version number and creation date of the currently running device software that the device loaded during the last system startup.

`enable`	To change to the Privileged EXEC mode.
`show system info`	To display the system information such as the version number and creation date of the currently running device software that the device loaded during the last system startup.

6.1 Loading a previous device 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.

If the Secure Boot function is active, then you cannot downgrade to a software version earlier than 10.3.00. See the *Basic Settings > Software* dialog, *Software update* frame.

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 device lets you update the device software, if a suitable device software image is saved on a storage medium which is accessible from your PC.

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

Perform the following steps:

- ☐ Navigate to the folder where the device software image is saved.
- ☐ Open the *Basic Settings > Software* dialog.
- ☐ Drag and drop the file into the area. As an alternative, click in the area to select the file.
- ☐ Start the software update. To do this, click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays a success notification.
    During the next startup, the device boots with the device software that you have transferred.

6.3 Software update from a server

The device lets you update its software if you have access to a server where a suitable device software image is saved.

The device gives you the following options to update the device software:
- Software update through FTP
- Software update through TFTP
- Software update through SFTP
- Software update through SCP

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

6.3.1 Software update through FTP

This option lets you update the device software with a software image the device retrieves from an FTP server.

Do not use this method if you transmit data over untrusted networks.

The prerequisite is that the access role `administrator` is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `ftp://user:password@IP_address:port/path/to/software_image.bin`
  You can also specify the URL without the user name and password. In this case, enter them in the *Credentials* window after clicking the *Start* button.
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote ftp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from an FTP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `ftp://user:password@10.0.1.159:21/path/to/software_image.bin`
  URL of the FTP server where the device software image file is saved.
  You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards.
  - `ftp://`
    Protocol for the file transfer
  - `user`
    User account name of the FTP server
  - `password`
    User account password
  - `10.0.1.159`
    IP address of the FTP server
  - `21`
    Default port for FTP
  - `/path/to/`
    The path to the device software image on the FTP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

6.3.2 Software update through TFTP

This option lets you update the device software with a software image the device retrieves from a TFTP server.

Do not use this method if you transmit data over untrusted networks.

The prerequisite is that the access role `administrator` is assigned to the user account you use to perform the actions on the device.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `tftp://IP_address/path/to/software_image.bin`
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote tftp://0.0.1.159/
path/to/software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from a TFTP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `tftp://10.0.1.159/path/to/software_image.bin`
  URL of the TFTP server where the device software image is saved.
  - `tftp://`
    Protocol for the file transfer
  - `10.0.1.159`
    IP address of the TFTP server
  - `/path/to/`
    The path to the device software image on the TFTP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

6.3.3 Software update through SFTP

This option lets you update the device software with a software image the device retrieves from an SFTP server.

Prerequisites:

- The access role `administrator` is assigned to the user account you use to perform the actions on the device.
- The SFTP server is known to the device. See the *Device Security > SSH Known Hosts* dialog.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `sftp://user:password@IP_address/path/to/software_image.bin`
  You can also specify the URL without the user name and password. In this case, enter them in the *Credentials* window after clicking the *Start* button.
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote sftp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from an SFTP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `sftp://user:password@10.0.1.159:21/path/to/software_image.bin`
  URL of the SFTP server where the device software image is saved.
  You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards.
  - `sftp://`
    Protocol for the file transfer
  - `user`
    User account name of the SFTP server
  - `password`
    User account password
  - `10.0.1.159`
    IP address of the SFTP server
  - `/path/to/`
    The path to the device software image on the SFTP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

6.3.4 Software update through SCP

This option lets you update the device software with a software image the device retrieves from an SCP server.

Prerequisites:
- The access role `administrator` is assigned to the user account you use to perform the actions on the device.
- The SCP server is known to the device. See the *Device Security > SSH Known Hosts* dialog.

Perform the following steps:

- ☐ Open the *Basic Settings > Software* dialog.
- ☐ In the *Software update* frame, *URL* field, specify the URL for the device software image using the following format:
  `scp://user:password@IP_address/path/to/software_image.bin`
  You can also specify the URL without the user name and password. In this case, enter them in the *Credentials* window after clicking the *Start* button.
- ☐ Click the *Start* button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays an information that the device software was successfully updated.
    During the next startup, the device boots with the device software that you have transferred.

```
enable

copy firmware remote scp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

To change to the Privileged EXEC mode.

To transfer the device software image from an SCP server to the flash memory of the device.

- `copy firmware remote`
  To copy the device software image from a remote location.
- `user:password@10.0.1.159:21/path/to/software_image.bin`
  URL of the SCP server where the device software image is saved.
  You can also specify the URL without the user name and password. In this case, the device will prompt you to enter the missing information afterwards.
  - `scp://`
    Protocol for the file transfer
  - `user`
    User account name of the SCP server
  - `password`
    User account password
  - `10.0.1.159`
    IP address of the SCP server
  - `/path/to/`
    The path to the device software image on the SCP server
  - `software_image.bin`
    Name of the device software image
- `system`
  To transfer the copied device software image to the flash memory.

6.4 Software update from the external memory (*ENVM*)

6.4.1 Manually—initiated by the administrator

The device lets you update the device software with a few mouse clicks, if a suitable device software image is saved on the selected external memory (*ENVM*).

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

Perform the following steps:

- ☐ Open the *Basic Settings > Load/Save* dialog.
- ☐ In the *External memory* frame, verify that the relevant external memory is selected from the *Selected external memory* drop-down list.
- ☐ Open the *Basic Settings > Software* dialog.
- ☐ Mark the table row for which the *File location* column displays the value `sd-card` or `usb`.
- ☐ Start the software update. To do this, click the ⬆ button.
  - The device transfers the previously used device software to the backup memory.
  - The device transfers the selected file to the flash memory, replacing the previously used device software.
    As soon as the update procedure is completed successfully, the device displays a success notification.
    During the next startup, the device boots with the device software that you have transferred.

6.4.2 Automatically—initiated by the device

When the following files are located in the external memory (*ENVM*) during the system startup, the device updates the device software automatically:

- the device software image
- a text file `startup.txt` with the content `autoUpdate=<software_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:

- ☐ Transfer the new device software image into the main directory of the external memory (*ENVM*). Use only a device software image suitable for the device.
- ☐ Create a text file `startup.txt` in the main directory of the external memory (*ENVM*).
- ☐ Open the `startup.txt` file in the text editor and add the following line:
  `autoUpdate=<software_image_file_name>.bin`
- ☐ Install the external memory (*ENVM*) in the device.
- ☐ Restart the device.
  During the booting process, the device checks automatically the following criteria:
  - Is an external memory (*ENVM*) connected?
  - Is a `startup.txt` file in the main directory of the external memory (*ENVM*)?

- Does the device software image exist which is specified in the `startup.txt` file?
- Is the version of the device software image more recent than the device software that the device is currently using?

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 device 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 a wrong device software image
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software update aborted because the device did not save the device software image.

7 Configuring the ports

The following port configuration functions are available.

- Enabling/Disabling the port
- Selecting the operating mode
- Gigabit Ethernet mode for ports

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.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no shutdown`	To enable the interface.

7.2 Selecting the operating mode

In the default setting, the ports are set to *Autoneg* 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 *Autoneg* column.
  - ☐ In the *Manual configuration* column, specify the desired operating mode (transmission rate, duplex mode).
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no auto-negotiate`	To disable the automatic configuration mode.
`speed 100 full`	To set port speed 100 Mbit/s and full-duplex.

7.3 Gigabit Ethernet mode for ports

The device supports 2.5 Gbit/s on several interfaces with one of the following SFP transceivers:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

The device supports 10 Gbit/s on several interfaces with one of the following SFP+ transceivers:
- M-SFP-10-SR/LC EEC
- M-SFP-10-LR/LC EEC
- M-SFP-10-ER/LC EEC
- M-SFP-10-ZR/LC

The type of the transceiver plugged into the slot determines the port speed. The device has no option to set the speed manually. Ports with 2.5 Gbit/s or 10 Gbit/s speed only support data rates of 1 Gbit/s and higher.

Depending on the hardware of the device, the actual usable data rate might be lower than the data rate that the media module supports.

Note:
For further information about the transceiver order numbers, see the “Accessories” chapter in the “Installation” user manual.

7.3.1 Checking port parameters

You use the Gigabit Ethernet mode to get a higher bandwidth for uplinks. To use this function, insert an applicable transceiver type in the appropriate slot.

Perform the following steps:

☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.

The column *Manual configuration* displays the value `2.5 Gbit/s FDX` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

The column *Manual configuration* displays the value `10 Gbit/s FDX` for the ports that have a 10 Gbit/s SFP+ transceiver inserted.

You cannot change the speed.

```
show port 1/1
```

To display the parameters for slot 1 port 1. The `Physical Mode` list entry displays the value `2500 full` for the ports that have a 2.5 Gbit/s SFP transceiver inserted.

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

```
show port 1/2
```

To display the parameters for slot 1 port 2. The `Physical Mode` list entry displays the value `10G full` for the ports that have a 10 Gbit/s SFP+ transceiver inserted.

```
Interface.....................1/2
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................10G full
Physical Status...............-
```

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 to reduce possible unauthorized access to the device.

- Changing the SNMPv1/v2 community
- Disabling write access for SNMPv1/v2
- Disabling SNMPv1/v2
- Disabling HTTP
- Using your own HTTPS certificate
- Using your own SSH key
- Disabling Telnet
- Disabling HiDiscovery
- Restricting access to device management
- Adjusting the session timeouts
- Deactivating the unused modules
- Customizing the SSH settings
- Making SSH hosts known to the device

8.1 Changing the SNMPv1/v2 community

SNMPv1 and SNMPv2 work unencrypted. Every SNMP packet contains the IP address of the sender and the plaintext *community name* with which the sender accesses the device. If the *SNMPv1* and/or *SNMPv2* function is active, then the device lets anyone who knows the *community name* access the device. Treat the *community names* with discretion.

The *community names* `public` for *read-only* access and `private` for *read and write* access are preset. If you are using SNMPv1 or SNMPv2, then change the default *community name*. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > SNMPv1/v2 Community* dialog. The dialog displays the communities that are set up.
- ☐ For the `Write` community, specify in the *Name* column the *community name*.
  - Up to 64 alphanumeric characters are allowed.
  - The device differentiates between upper and lower case.
  - Specify a different *community name* than for *read-only* access.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp community rw <community name>`	To specify the community for *read and write* access.
`show snmp community`	To display the communities that have been set up.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

8.2 Disabling write access for SNMPv1/v2

To reduce possible unauthorized access to the device, you can disable the write access for the `Write` community, while the *read-only* access remains enabled. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > SNMPv1/v2 Community* dialog, *Configuration* tab.
- ☐ Deactivate the write access for the `Write` community. To do this, mark the *SNMP V1/V2 readOnly* checkbox.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`snmp community rw private read-only`	To deactivate the write access for the `private` community.
`show snmp community`	To display the SNMP access mode of the SNMPv1/v2 communities.

```
SNMP V1/V2 community     Access mode
--------------------     -----------
public                   read-only
private                  read-only
```

`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

8.3 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.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no snmp access version v1`	To deactivate the SNMPv1 protocol.
`no snmp access version v2`	To deactivate the SNMPv2 protocol.
`show snmp access`	To display the SNMP server settings.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

8.4 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.
- ☐ Disable the *HTTP* protocol.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no http server`	To disable the HTTP protocol.

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:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https server`	To enable the HTTPS protocol.

8.5 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.
- ☐ Disable the *Telnet* server.
  Select the *Off* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no telnet server`	To disable the Telnet server.

If the *SSH* server is disabled and you also disable the *Telnet* server, then access to the device management is only possible using the Command Line Interface through the serial connection. 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.
- ☐ Enable the *SSH* server.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh server`	To enable the SSH server.

8.6 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.
- ☐ Disable HiDiscovery access completely.
  Select the `Off` radio button in the *HiDiscovery protocol v1/v2* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`network hidiscovery mode read-only`	To disable write permission of the HiDiscovery software.
`no network hidiscovery operation`	To disable HiDiscovery access.

8.7 Restricting access to device management

In the default setting, everyone can access the device management from any IP address using any protocol. The device lets you restrict access to device management for selected protocols from a specific IP address range.

8.7.1 Restricting access from a specific IP address range

In the following 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 18: Parameters for the IP access restriction

Parameter	Company network	Mobile phone network
Network address	`192.168.1.0`	`109.237.176.0`
Netmask	`24`	`24`
Desired protocols	https, snmp	ssh

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.

Note:
Before you enable the access restriction, verify that the table contains at least one active rule that grants you access to the device management. Otherwise, access to the device management is only possible using the Command Line Interface through the serial connection.

- ☐ Enable the access restriction.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`show network management access global`	To display if the access restriction is enabled or disabled.
`show network management access rules`	To display the entries that have been configured.
`no network management access operation`	To disable the IP access restriction.
`network management access add 2`	To add a rule with index `2` for the address range of the company network.
`network management access modify 2 ip 192.168.1.0`	To specify the IP address of the company network.
`network management access modify 2 mask 24`	To specify the netmask of the company network.
`network management access modify 2 ssh disable`	To deactivate SSH for the address range of the company network. Repeat the operation for every unwanted protocol.
`network management access add 3`	To add a rule with index `3` for the address range of the mobile phone network.
`network management access modify 3 ip 109.237.176.0`	To specify the IP address of the mobile phone network.
`network management access modify 3 mask 24`	To specify the netmask of the mobile phone network.
`network management access modify 3 snmp disable`	To deactivate SNMP for the address range of the mobile phone network. Repeat the operation for every unwanted protocol.
`no network management access status 1`	To deactivate the default entry. This entry lets users have access to the device from any IP address and the supported protocols.
`network management access status 2`	To activate the rule with index `2` for the address range of the company network.
`network management access status 3`	To activate the rule with index `3` for the address range of the mobile phone network.
`show network management access rules`	To display the entries that have been configured.
`network management access operation`	To enable the access restriction.

8.8 Adjusting the session timeouts

The device lets you automatically terminate the session upon inactivity of the user that is logged in. 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 the 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.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh timeout <0..160>`	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.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`telnet timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using a Telnet connection.

Timeout for Command Line Interface sessions using the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`cli serial-timeout <0..160>`	To specify the timeout period in minutes for Command Line Interface sessions using the 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`network management access web timeout <0..160>`	To specify the timeout period in minutes for Graphical User Interface sessions

8.9 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.
- ☐ Apply the settings temporarily. To do this, click the  button.

8.10 Customizing the SSH settings

In the state on delivery, the built-in SSH server of the device uses a self-signed RSA *host key*. To increase the security level of SSH connections to the device, you can replace the RSA *host key* in the device in the following ways:

- "Generating the RSA host key in the device" on page 144
- "Transferring an externally generated private RSA key to the device" on page 145

8.10.1 Generating the RSA host key in the device

The device lets you generate an RSA *host key* directly in the device and thus replace the stored RSA *host key*. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ Disable the *SSH* server.
  To do this, in the *Operation* frame, select the *Off* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the *Signature* frame, click the *Create* button.
  Generating the new RSA *host key* starts.

  You can monitor the process when you click the ↻ button. When the value in the *Oper status* field changes from *rsa* to *none*, the process is complete.
- ☐ Enable the *SSH* server.
  To do this, in the *Operation* frame, select the *On* radio button.
  The generated RSA *host key* is immediately active.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the *SSH* server.
`ssh key rsa generate`	To generate the new RSA *host key*. This process takes a few seconds and finishes without feedback. You can monitor the process when you execute the `show ssh server` command. When the value in the `SSH key operation status` line changes from `rsa` to `none`, the process is complete.
`ssh server`	To enable the *SSH* server. The generated RSA *host key* is immediately active.

8.10.2 Transferring an externally generated private RSA key to the device

Network administrators can generate an RSA *host key* outside the device, for example, by using the `ssh-keygen` command, which is part of OpenSSH. Optionally, you can have the externally generated RSA key signed by a Certification Authority (CA).

To generate an RSA key outside the device, enter the following command on the management station: `ssh-keygen -b 4096 -t rsa -m PEM -N '' -f key_name`

- `-b 2048`
  Length of the key
- `-t rsa`
  Type of the key
- `-m PEM`
  Format of the key
- `-N ''`
  Passphrase
- `-f key_name`
  File name of the key
  Replace the string `key_name` with the desired file name.

After the command has completed, you find the following files in the file system of the management station:

- Private key (`key_name` without file extension)
  This key enables the SSH server in the device to authenticate itself to the SSH clients. You transfer this key to the device in the further process. Keep the private key in an trusted, secure location, but not in a publicly accessible or shared location.
- Public key (`key_name` with the file extension `.pub`)
  This key enables SSH clients to verify the authenticity of the SSH server in the device.

You can transfer the externally generated private key to the device using one of the following options:

- Importing the private key from the management station or a file server directly into the device using the Graphical User Interface or the Command Line Interface.
  See “Importing the private key directly into the device” on page 145.
- Transferring the private key to the device through the external memory using the Command Line Interface.
  See “Transferring the private key to the device through the external memory” on page 146.

Importing the private key directly into the device

You can import the private key from the management station or a file server directly into the device using the Graphical User Interface or Command Line Interface. Confirm that the private key resides on the file server for the shortest time necessary during the transfer. Immediately after the transfer, relocate the private key to a location that is inaccessible from the network.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *SSH* tab.
- ☐ Disable the *SSH* server.
  To do this, in the *Operation* frame, select the *Off* radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

- ☐ Import the private key:
  - ☐ When the file is located on your PC or on a network drive, drag and drop it onto the  area. As an alternative, click in the area to select the file.
  - ☐ If the file is on an FTP server, then specify the URL in the following form:
    `ftp://<user>:<password>@<IP address>[:port]/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ If the file is on a TFTP server, then specify the URL in the following form:
    `tftp://<IP address>/<path>/<file name>`
    Do not use this method if you transmit data over untrusted networks.
  - ☐ If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:
    `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 into the server.
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
    Remember to make the SCP or SFTP server known to the device before the device accesses the server for the first time. See the *Device Security > SSH Known Hosts* dialog.
- ☐ Click the *Start* button.
  The file transfer starts. This process takes a few seconds.
- ☐ Relocate the private key to a location that is inaccessible from the network.
- ☐ Enable the *SSH* server.
  To do this, in the *Operation* frame, select the *On* radio button.
  The imported private key is immediately active.
- ☐ Apply the settings temporarily. To do this, click the  button.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost.

`enable`	To change to the Privileged EXEC mode.
`copy sshkey remote scp://192.168.1.1/path/to/priv_key_file nvm`	To import the private key from a management station with the IP address 192.168.1.1 using SCP. Immediately after the transfer, relocate the private key to a location that is inaccessible from the network.
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the *SSH* server.
`ssh server`	To enable the *SSH* server. The imported private key is immediately active.

Transferring the private key to the device through the external memory

You can transfer the private key to the device through the external memory using the Command Line Interface.

Preparatory steps:

- ☐ On the management station, copy the private key to the external memory connected to the management station. Confirm that the private key resides on the external memory for the shortest time necessary during the transfer. Immediately after the transfer, wipe the private key from the external memory.
- ☐ Plug the external memory into the device.

Execute the following commands only if you are connected to the device management through the serial connection. If you are connected through SSH, the connection to the device management will be lost.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`copy sshkey envm path/to/priv_key_file nvm`	To transfer the private key to the device through the external memory (*ENVM*). Immediately after the transfer, wipe the private key from the external memory (*ENVM*).
`configure`	To change to the Configuration mode.
`no ssh server`	To disable the *SSH* server.
`ssh server`	To enable the *SSH* server. The imported private key is immediately active.

8.11 Making SSH hosts known to the device

The device permits SSH-based connections only to remote servers that are known to the device. In the state on delivery, no remote server is set up as a known host on the device.

When downloading a device software image or importing a configuration profile through SCP or SFTP, these protocols use an underlying SSH connection. For SSH, you make remote servers known by using their public key fingerprint. The device verifies the identity of the remote server by comparing the public key fingerprint stored on the device with the fingerprint calculated from the public key which the remote server actually sent. If the calculated public key fingerprint does not match the stored public key fingerprint, the device terminates the connection.

You can find out the public key fingerprint of the remote server and the key type, as follows:
- From the administrator of a known SSH server.
  Use a trustworthy channel for receiving this data.
- From the error message following an unsuccessful software update in the *Software* dialog.
  This happens because of the mismatch between the public key fingerprint stored in the device and the fingerprint calculated from the public key which the remote server actually sent.

The device provides the following setting options:
- Adding an SSH Known Hosts entry
- Updating an SSH Known Hosts entry
- Deactivating an SSH Known Hosts entry
- Deleting an SSH Known Hosts entry

Adding an SSH Known Hosts entry

You can set up a maximum of 50 entries containing the server address and the public key fingerprint. If a remote server has several keys set up, for different encryption algorithms, add each of the public key fingerprints as a separate entry.

Verify that the public key fingerprints you store on the device are from a trustworthy source, the SSH server administrator, for example.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ In the *Index* field, specify the index value. Assign a unique value.
- ☐ In the *Address* field, specify the IPv4 or IPv6 address, or the DNS hostname of the remote server.
- ☐ In the *Key fingerprint* field, enter the public key fingerprint of the remote server.
- ☐ From the *Key type* drop-down list, select the corresponding key type. This is the algorithm that the administrator of the remote server used to generate the server key pair.
- ☐ Click the *Ok* button.
  The device adds a table row.
  The device accepts establishing a connection to the remote server from now on.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts add {index} address {ipv4 | ipv6 | dns} key-type {rsa | dsa | ecdsa | ed25519} key-fingerprint {string_base64}`	To add an entry with index, address of the remote server, key type, and public key fingerprint of the remote server.
`show ssh known-hosts`	To display the set up entries.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 107.

Updating an SSH Known Hosts entry

If the public key of the remote server changes, then you need to update the fingerprint in the respective table row.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog.
- ☐ Unmark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the *Key fingerprint* column, enter the new public key fingerprint of the remote server.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ To activate the entry, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts modify {index} status disable`	To deactivate the entry.
`ssh known-hosts modify {index} key-fingerprint {string_base64}`	To modify the entry with the index number you have entered.
`ssh known-hosts modify {index} status enable`	To activate the entry.
`show ssh known-hosts {index}`	To check the updated entry.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 107.

Deactivating an SSH Known Hosts entry

You deactivate an entry, for example, when the current server key will soon become invalid due to the rotation of the server key.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog.
- ☐ In the table row for the relevant entry, unmark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts modify {index} status disable`	To deactivate the entry with the index number you have entered.
`show ssh known-hosts {index}`	To check if the entry is inactive.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 107.

Deleting an SSH Known Hosts entry

If the device is no longer permitted to contact a remote server or the public key is no longer valid, then you can delete the corresponding entry.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog.
- ☐ In the table row for the relevant entry, mark the checkbox in the *Index* column.
- Click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`ssh known-hosts delete {index}`	To delete the entry with the index number you have entered.
`show ssh known-hosts {index}`	To check if the entry has been deleted.

`SSH known hosts information`
`---------------------------`
`No entry.`	

`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 107.

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 generate 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

Denial of Service (DoS) is a cyberattack that aims to make certain services or devices unusable. 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 the network against invalid or falsified data packets targeted at certain services or devices. You have the option of specifying filters 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 options:
- 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:
- Activating the Null Scan filter function
- Activating the Xmas filter function
- Activating the SYN/FIN filter function
- Activating the TCP Offset protection function
- Activating the TCP SYN protection function
- Activating the L4 Port protection function
- Activating the Min. Header Size filter function

Activating 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.
- ☐ Apply 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-null`	To activate the *Null Scan filter* function.
`no dos tcp-null`	To deactivate the *Null Scan filter* function.

Activating 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.
- ☐ Apply 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-xmas`	To activate the *Xmas filter* function.
`no dos tcp-xmas`	To deactivate the *Xmas filter* function.

Activating 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.
- ☐ Apply 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-syn-fin`	To activate the *SYN/FIN filter* function.
`no dos tcp-syn-fin`	To deactivate the *SYN/FIN filter* function.

Activating 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.
- ☐ Apply 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-offset`	To activate the *TCP Offset protection* function.
`no dos tcp-offset`	To deactivate the *TCP Offset protection* function.

Activating 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 (layer 4) 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.
- ☐ Apply 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-syn`	To activate the *TCP SYN protection* function.
`no dos tcp-syn`	To deactivate the *TCP SYN protection* function.

Activating 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.
- ☐ Apply 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 l4-port`	To activate the *L4 Port protection* function.
`no dos l4-port`	To deactivate the *L4 Port protection* function.

Activating the Min. Header Size filter function

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.

If the received packet is the first fragment that the device detects, then the device discards the data packet.

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.
- ☐ Apply 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:
- Activating the Land Attack filter function

Activating 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:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Land Attack filter* function. To do this, in the *IP* frame, mark the *Land Attack filter* checkbox.
- ☐ Apply 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 ip-land enable`	To activate the *Land Attack filter* function.
`no dos ip-land disable`	To deactivate the *Land Attack filter* function.

9.1.3 Filters for ICMP packets

To selectively process *ICMP* packets, the device offers you the following filters:
- Activating the Fragmented packets filter function
- Activating the Packet size filter function
- Activating the Drop broadcast ping function

Activating 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:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Fragmented packets filter* function. To do this, in the *ICMP* frame, mark the *Fragmented packets filter* checkbox.
- ☐ Apply 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 icmp-fragmented`	To activate the *Fragmented packets filter* function.
`no dos icmp-fragmented`	To deactivate the *Fragmented packets filter* function.

Activating 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:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Packet size filter* function. To do this, in the *ICMP* frame, mark the *Packet size filter* checkbox.
- ☐ Apply 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 icmp payload-check`	To activate the *Packet size filter* function.
`no dos icmp payload-check`	To deactivate the *Packet size filter* function.

Activating the Drop broadcast ping function

The *Drop broadcast ping* function helps protect the network from broadcast ping attacks, also known as ICMP Smurf attacks. With the Broadcast ping method, the attacker floods a target device (the victim) by sending a large number of *ICMP echo request* packets to the IPv4 broadcast address. These packets contain a spoofed IP source address which is the IP address of the victim. Stations responding to the Broadcast ping send their replies to the victim, thus flooding the victim and possibly causing instability.

The device uses the *Drop broadcast ping* function to discard the Broadcast pings.

In the default setting, the *Drop broadcast ping* function is disabled. To activate the *Drop broadcast ping* function, perform the following steps:

- ☐ Open the *Network Security > DoS > Global* dialog.
- ☐ Activate the *Drop broadcast ping* function. To do this, in the *ICMP* frame, mark the *Drop broadcast ping* checkbox.
- ☐ Apply 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 icmp-smurf-attack`	To activate the *Drop broadcast ping* function.
`no dos icmp-smurf-attack`	To deactivate the *Drop broadcast ping* function.

9.2 ACL

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)
- Type of the transmitting protocol (MAC/IPv4)
- Source or destination port of a data packet (IPv4)
- Service class of a packet (MAC)
- Membership of a specific VLAN (MAC)
- DSCP classification (IPv4)
- ToS classification (IPv4)
- Packet Fragmentation (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 port or LAG, 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 416.

Note:
You can assign a single ACL to any number of ports or VLANs.

Note:
If you activate the *Packet fragmented* function for a rule, then the rule processes IPv4 fragments with the offset other than zero. The rule processes every IPv4 fragment except for the initial IPv4 fragment.

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:
- add 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

Note:
You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

Perform the following steps:

- ☐ Open the *Network Security > ACL > IPv4 Rule* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ Click the *Group name* drop-down list to specify the ACL (group) name.
  Enter the name in the search box.
  - ☐ To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  - ☐ To add a name: Enter the name in the search box, then click the *Create* link below the search box.
- ☐ 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.
- ☐ Apply 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 set up ACLs to block the communication from computers B and C to computer A, based on the IP address (TCP/UDP port, etc.).

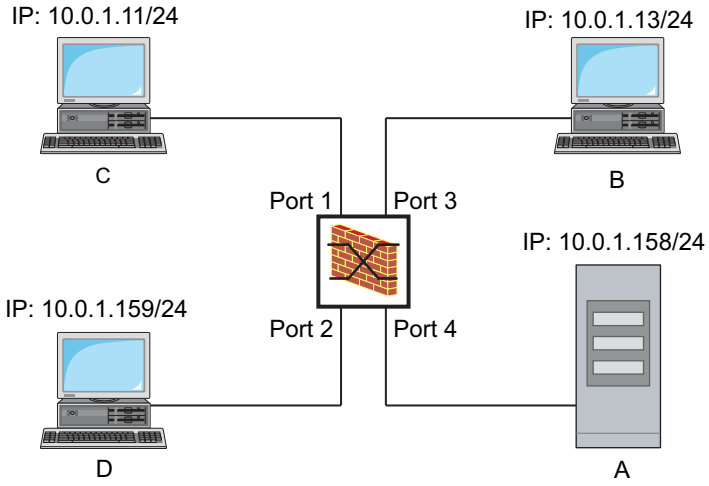


Figure 18: Application example of an IP ACL

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`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 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 permit src any dst any`	To add a rule to the IP ACL admitting IP data packets.
`show access-list ip filter1`	To display the rules of the IP ACL `filter1`.
`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 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).
`show access-list ip filter2`	To display the rules of the IP ACL `filter2`.

9.2.3 Creating and editing MAC rules

When filtering MAC data packets, the device lets you:

- add 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.
- ☐ Click the *Group name* drop-down list to specify the ACL (group) name.
  Enter the name in the search box.
  - ☐ To use an existing name: Enter the name in the search box, then select the desired item from the search results.
  - ☐ To add a name: Enter the name in the search box, then click the *Create* link below the search box.
- ☐ 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.
- ☐ Apply 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:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mac acl add 1 macfilter`	To add an MAC ACL with the ID `1` and the name `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	To add a rule to position `1` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	To add a rule to position `2` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	To add a rule to position `3` of the MAC ACL with the ID `1` rejecting packets with EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	To add a rule to position `4` of the MAC ACL with the ID `1` forwarding packets.
`show acl mac rules 1`	To display the rules of the MAC ACL with the ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	To change to the Interface Configuration mode of the interfaces `1/1` to `1/6`.

`acl mac assign 1 in 1`	To assign the MAC ACL with the ID `1` to incoming data packets (`1/1`) on interfaces `1/6` to `in`.
`exit`	To leave the interface mode.
`show acl mac assignment 1`	To display the assignment of the MAC ACL with the ID `1` to interfaces or VLANs.

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 direction.
- To select the ACL using the group name.

Perform the following steps:

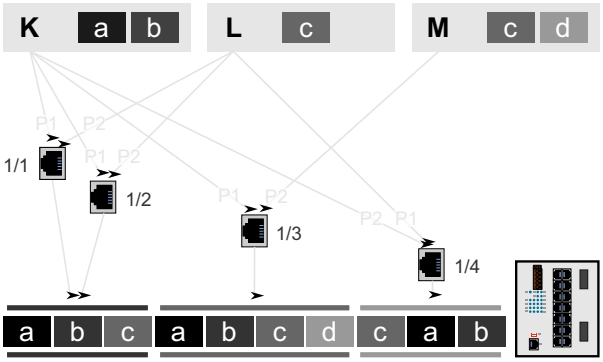
- ☐ Open the *Network Security > ACL > Assignment* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Port/VLAN* field, specify the desired port or the desired VLAN.
  - ☐ In the *Priority* field, specify the priority.
  - ☐ In the *Direction* field, specify the data 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.
- ☐ Apply the settings temporarily. To do this, click the button.

9.2.6 Maximum number of rules that can be assigned

The device lets you specify a maximum of 100 ACLs, which can each contain a certain number of rules. The number of rules that you can actually assign to the ports and VLANs might be smaller than the number of rules specified in the device. The following example illustrates the factors that affect the possible number that you can actually assign.

In the device, 3 ACLs with a total of 4 rules are specified:
- ACL K containing the rules a and b
- ACL L containing the rule c
- ACL M containing the rules c and d

The ACLs and rules have symbolic names. Rules with the same name contain the same settings.



When assigning the ACLs to ports 1/1 to 1/4, the device writes the rules contained in that ACLs with the specified priority to a hardware memory area that the ports and VLANs share. The order of the rules in relation to each other is determined by the index number within the respective ACL and by the assignment priority.

- Ports 1/1 and 1/2
  Each port is assigned 3 identical rules. The order is the same because of the assignment priority.
  The device writes 3 rules to the hardware memory. Both ports share these rules.
- Port 1/3
  The first 3 rules are identical to those for port 1/1.
  The device writes the 3 rules again to the hardware memory, along with the additional fourth rule.
- Port 1/4
  The rules are identical to those for port 1/1.
  The device writes the 3 rules again to the hardware memory due to the changed order.

Port	Assigned ACLs	Applied Rules	Number of Rules	Occupied Memory
1/1	K, L	a, b, c	3	3
1/2	K, L	a, b, c	0	3
1/3	K, M	a, b, c, d	4	7
1/4	L, K	c, a, b	3	10

Conclusion: Due to slight differences when assigning, 4 rules occupy the memory of 10 rules. You can optimize the occupied memory by smartly organizing the rules yourself.

9.3 MAC authentication bypass

The *MAC authorized bypass* function lets clients that do not support 802.1X, such as printers and fax machines, authenticate to the network using their MAC address. The device lets you specify the format of the MAC address used to authenticate the clients on the RADIUS server.

Example:

Split the MAC address into 6 groups of 2 characters. Use uppercase letters and a colon character as separator: `AA:BB:CC:DD:EE:FF`

Use the password `xY-45uM_e`. To do this, perform the following steps:

- ☐ Open the *Network Security > 802.1X > Global* dialog.
  In the *MAC authentication bypass format options* frame, perform the following steps:
- ☐ From the *Group size* drop-down list, select the item `2`.
  The device splits the MAC address into 6 groups of 2 characters.
- ☐ From the *Group separator* drop-down list, select the item `:`.
- ☐ From the *Upper or lower case* drop-down list, select the item *upper-case*.
- ☐ In the *Password* field, enter the password `xY-45uM_e`.
  The device uses this password for every client that authenticates to the RADIUS server. If you leave the field empty, then the device uses the formatted MAC address also as the password.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1x mac-authentication-bypass format group-size 2`	To specify the group size `2`.
`dot1x mac-authentication-bypass format group-separator :`	To specify the group separator `:`.
`dot1x mac-authentication-bypass format letter-case upper-case`	To specify that the device formats the authentication data in uppercase letters.
`dot1x mac-authentication-bypass password xY-45uM_e`	To specify the password `xY-45uM_e`. The device uses this password to authenticate every client on the RADIUS server.

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
- Differentiated services
- 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 (forwarding database).

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 corrupt 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 (forwarding database). When the MAC address of the sender is unknown, the device generates an entry. The device then compares the destination MAC address of the data packet with the entries stored in the MAC address table (forwarding database):
- 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 (forwarding database) by the device. A reboot or resetting the MAC address table (forwarding database) deletes the entries in the MAC address table (forwarding database).

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 set up and survive resetting of the MAC address table (forwarding database) 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 *MAC address* field, specify the destination MAC address.
– In the *VLAN ID* field, specify the VLAN ID.
– 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 *MAC address* field, select only one port.
  When you have defined a Multicast MAC address in the *MAC 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.

☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mac-filter <MAC address> <VLAN ID>`	To add the MAC address filter, consisting of a MAC address and VLAN ID.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`mac-filter <MAC address> <VLAN ID>`	To assign the port to a previously added MAC address filter.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

☐ 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 *Static* in the *Status* column.

☐ Apply 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 *Static* in the *Status* column, then click the button.

☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	To cancel the assignment of the MAC address filter on the port.
`exit`	To change to the Configuration mode.
`no mac-filter <MAC address> <VLAN ID>`	To delete the MAC address filter, consisting of a MAC address and a VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`save`	To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

☐ Delete learned MAC addresses.

☐ To delete the learned addresses from the MAC address table (forwarding database), click the button.
As an alternative, open the *Basic Settings > Restart* dialog and click the *Clear FDB* button.

`clear mac-addr-table`	To delete the learned MAC addresses from the MAC address table (forwarding database).

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 packets. 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 data streams between the Multicast routers and the monitors. The switches in the network between the Multicast routers and the monitors monitor the IGMP data packets continuously (IGMP Snooping).

Switches register logins for receiving a Multicast stream (IGMP report). The device then adds an entry in the MAC address table (forwarding database) 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 data packets and optimizing its own transmission settings for these data packets.

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 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 (forwarding database). 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.
- ☐ Enable the *IGMP Snooping* 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.
- ☐ Apply 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.
- ☐ Apply 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Setting the IGMP querier function

The device itself optionally sends active query messages. As an alternative, the device responds to query messages or detects other Multicast queriers in the network (*Querier* function).

Prerequisite:

The *IGMP Snooping* function is globally enabled.

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 *IP 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.
- ☐ Apply 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` (for learned).
- *Learn by LLDP*
  A port with this setting automatically discovers other Hirschmann devices using the Link Layer Discovery Protocol (LLDP). The device then learns the IGMP query status of this port from these Hirschmann devices and sets up 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` (for 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 globally enabled.

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Snooping Enhancements* dialog.
- ☐ Double-click the desired port in the desired VLAN.

- ☐ To activate one or more functions, select the corresponding options.
- ☐ Click the *Ok* button.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`igmp-snooping vlan-id 1 forward-all 1/1`	To activate the `Forward All` function for port `1/1` in VLAN `1`.

Setting up Multicasts

The device lets you set up 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 multicast data 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 19: Multicast IP addresses ignored by IGMP Snooping

Multicast IP address(es)	Multicast MAC address(es)	Protocols (Block)
224.0.0.0..224.0.0.255	01:00:5e:00:00:00..01:00:5e:00:00:ff	Local Network Control Block
224.0.1.1	01:00:5e:00:01:01	NTP/SNTP (Internetwork Control Block)
224.0.1.129..224.0.1.132	01:00:5e:00:01:81..01:00:5e:00:01:84	PTP (Internetwork Control Block)
239.255.16.12	01:00:5e:7f:10:0c	HiDiscovery v2 (Administratively Scoped Block)

Note:
According to RFC 1112 (*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 globally enabled.

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.
- ☐ Apply the settings temporarily. To do this, click the button.

10.3 Rate limiter

The rate limiter function helps ensure stable operation even with high data volumes by limiting the amount of data packets on the ports. The rate limitation is performed individually for each port, as well as separately for inbound and outbound data packets.

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 data packets.

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 amount of outbound data packets instead of the inbound data packets. 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 separated according to the type of the data packets:
  - 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 *Unit* column, you specify if the device interpretes the threshold values as percent of the port bandwidth or as packets per second. The threshold value `0` deactivates the rate limiter.

☐ Apply 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 packets with lower priority from interfering with delay-sensitive data packets. Delay-sensitive data packets include, for example, voice, video, and real-time data.

10.4.1 Description of prioritization

For data packet 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 packets of this *traffic class*, although there is a great deal of data packets in higher *traffic classes*.

10.4.2 Handling of received priority information

Applications label data packets with the following prioritization information:

- VLAN priority according to IEEE 802.1Q (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, IEEE 802.1Q 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”).

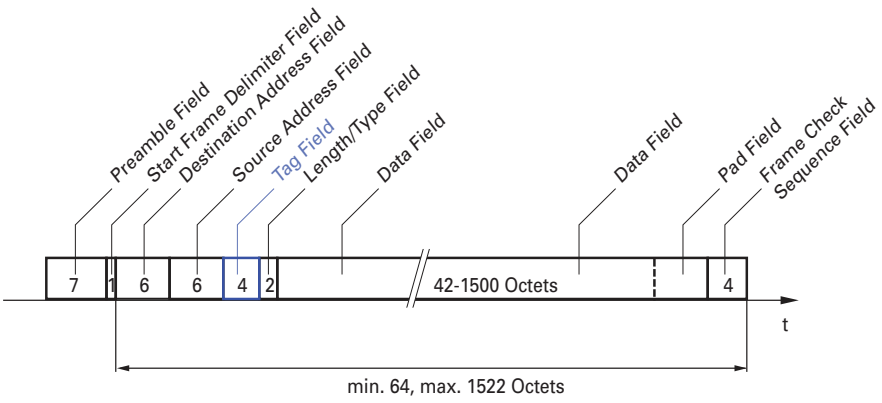


Figure 19: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the following information:
- Priority information
- When VLANs are set up, VLAN tagging

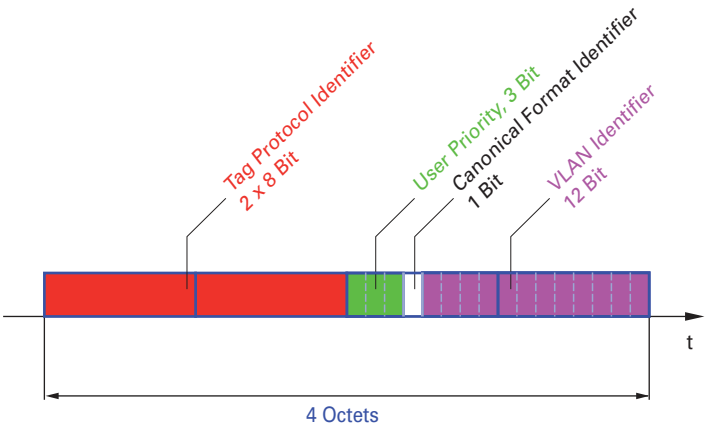


Figure 20: Structure of the VLAN tagging

A data packets with VLAN tag containing priority information but no VLAN information (VLAN ID = 0), is known as a *Priority Tagged* frame.

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.

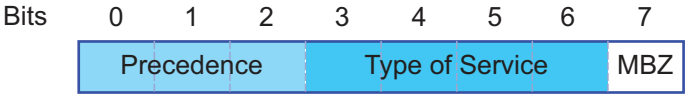


Table 20: ToS field in the IP header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	

Table 20: ToS field in the IP header (cont.)

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

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 data packets waiting to be sent on this port, then the device does not send data 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

Queue Shaping

Queue Shaping throttles the rate at which queues transmit packets. For example, using Queue Shaping, you rate-limit a higher strict-priority queue so that it lets a lower strict-priority queue to send packets even though higher priority packets are still available for transmission. The device lets you setup Queue Shaping for any queue. You specify Queue Shaping as the maximum rate at which the data packets pass through a queue by assigning a percentage of the available bandwidth.

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 *Weighted Fair Queuing* for *Traffic class* = `3`, 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* and Queue Shaping for *Traffic class* = `4`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
  - In the *Max. bandwidth [%]* column, specify the value `10`.

  When using a *Weighted Fair Queuing* and Queue Shaping combination for a specific *traffic class*, specify a higher value in the *Max. bandwidth [%]* column than the value specified in the *Min. bandwidth [%]* column.
- ☐ To activate *Weighted Fair Queuing* for *Traffic class* = `5`, 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* = `6`, proceed as follows:
  - Unmark the checkbox in the *Strict priority* column.
  - In the *Min. bandwidth [%]* column, specify the value `10`.
- To activate *Strict Priority* and Queue Shaping for *Traffic class* = `7`, proceed as follows:
  - Mark the checkbox in the *Strict priority* column.
  - In the *Max. bandwidth [%]* column, specify the value `10`.
- Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`cos-queue weighted 0`	To enable *Weighted Fair Queuing* for *traffic class* `0`.
`cos-queue min-bandwidth: 0 5`	To assign a weight of `5` % to *traffic class* `0`.
`cos-queue weighted 1`	To enable *Weighted Fair Queuing* for *traffic class* `1`.
`cos-queue min-bandwidth: 1 20`	To assign a weight of `20` % to *traffic class* `1`.
`cos-queue weighted 2`	To enable *Weighted Fair Queuing* for *traffic class* `2`.
`cos-queue min-bandwidth: 2 30`	To assign a weight of `30` % to *traffic class* `2`.
`cos-queue weighted 3`	To enable *Weighted Fair Queuing* for *traffic class* `3`.
`cos-queue min-bandwidth: 3 20`	To assign a weight of `20` % to *traffic class* `3`.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combining Weighted Fair Queuing and Queue Shaping

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`cos-queue weighted 4`	To enable *Weighted Fair Queuing* for *traffic class* `4`.
`cos-queue min-bandwidth: 4 10`	To assign a weight of `10` % to *traffic class* `4`.
`cos-queue max-bandwidth: 4 10`	To assign a weight of `10` % to *traffic class* `4`.
`cos-queue weighted 5`	To enable *Weighted Fair Queuing* for *traffic class* `5`.
`cos-queue min-bandwidth: 5 5`	To assign a weight of `5` % to *traffic class* `5`.

```
cos-queue weighted 6
```
To enable *Weighted Fair Queuing* for *traffic class* 6.

```
cos-queue min-bandwidth: 6 10
```
To assign a weight of 10 % to *traffic class* 6.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Setting up Queue Shaping

Perform the following steps:

```
enable
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
cos-queue max-bandwidth: 7 10
```
To assign a weight of 10 % to *traffic class* 7.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Management prioritization

The device lets you prioritize the management packets so that you can access the device management at any time in situations with high network load.

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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`vlan priority 3`	To assign interface `1/1` the *Port priority* `3`.
`exit`	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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`classofservice dot1p-mapping 0 2`	To assign a VLAN priority of `0` to *traffic class* `2`.
`classofservice dot1p-mapping 1 2`	To assign a VLAN priority of `1` to *traffic class* `2`.
`exit`	To change to the Privileged EXEC mode.
`show classofservice dot1p-mapping`	To display the assignment.

Assigning Port priority to received data packets

Perform the following steps:

```
enable
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
interface 1/1
```
To change to the Interface Configuration mode of interface `1/1`.

```
classofservice trust  untrusted
```
To assign the *`untrusted`* mode to the interface.

```
classofservice  dot1p-mapping 0 2
classofservice  dot1p-mapping 1 2
```
To assign a VLAN priority of `0` to *traffic class* `2`.
To assign a VLAN priority of `1` to *traffic class* `2`.

```
vlan priority 1
```
To specify the value `1` for the *Port priority*.

```
exit
```
To change to the Configuration mode.

```
exit
```
To change to the Privileged EXEC mode.

```
show classofservice trust
```
To display the Trust mode of the ports/interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
configure
```
To change to the Configuration mode.

```
classofservice  ip-dscp-mapping cs1 1
```
To assign the DSCP value `CS1` to *traffic class* `1`.

```
show classofservice  ip-dscp-mapping
```
To display the IP DSCP assignments

```
    IP DSCP       Traffic Class
-------------     -------------
  be                   2
  1                    2
  .                    .
  .                    .
  (cs1)                1
  .                    .
```

Assigning the DSCP priority to received IP data packets

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`classofservice trust ip-dscp`	To assign the `trust ip-dscp` mode globally.
`exit`	To change to the Configuration mode.
`show classofservice trust`	To display the Trust mode of the ports/interfaces.

```
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

Configuring traffic shaping on a port

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`traffic-shape bw 50`	To limit the maximum bandwidth of the port `1/2` to 50%.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show traffic-shape`	To display the Traffic Shaping configuration.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
network management priority dot1p 7
```
To assign the VLAN priority of 7 to management packets. The device sends management packets with the highest priority.

```
show network parms
```
To display the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Configuring Layer 3 management priority

Perform the following steps:

- ☐ Open the *Switching > QoS/Priority > Global* dialog.
- ☐ In the *IP DSCP value for management packets* field, specify the DSCP value with which the device sends management data packets.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
network management priority ip-dscp 56
```
To assign the DSCP value of 56 to management packets. The device sends management packets with the highest priority.

```
show network parms
```
To display the priority of the VLAN in which the device management is located.

```
IPv4 Network
------------
...
Management IP-DSCP value....................56
```

10.5 Differentiated services

RFC 2474 defines the “Differentiated Services” field in the IP header. This field is also called “DiffServ Codepoint” or DSCP. The DSCP field is used for classification of packets into different quality classes.

The DSCP field replaces the ToS field. The first 3 bits of the DSCP field are used to divide the packets into classes. The next 3 bits are used to further subdivide the classes on the basis of different criteria. This results in up to 64 different service classes.

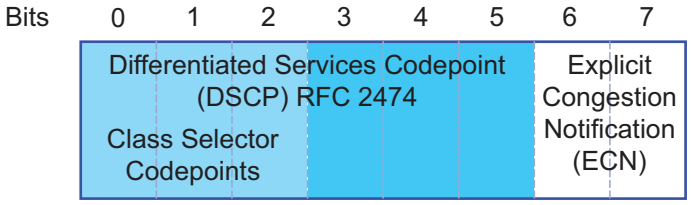


Figure 21: Differentiated Services field in the IP header

The different DSCP values get the device to employ a different forwarding behavior, what is known as *Per Hop Behavior (PHB)*. The following PHB classes are defined:

- Class Selector (CS0–CS7)
  For backward compatibility, the *Class Selector* PHB assigns the 7 possible *IP Precedence* values from the previous ToS field to specific DSCP values.
- Expedited Forwarding (EF)
  For applications with high priority. The *Expedited Forwarding* PHB reduces delays (latency), jitter, and packet loss (RFC 2598).
- Assured Forwarding (AF)
  The *Assured Forwarding* PHB provides a differentiated schema for handling different data packets (RFC 2597).
- Default Forwarding/Best Effort
  This PHB stands for the dispensation with a specific prioritization.

Table 21: Assigning the IP precedence values to the DSCP value

ToS Meaning	Precedence Value	Assigned DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immediate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

10.5.1 Application example for the DiffServ function

Set up the device to drop packets received on port `1/1` with the source IP address `10.20.10.11`, the TCP protocol and the source port `80` using the following steps.

Perform the following steps:

☐ Step 1: Add a class.

☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *Class* dialog.

☐ Create a class:

– Click the button.
The dialog displays the *Create* window.
– In the *Class name* field, enter the name `class1`.
– From the *Type* drop-down list, select the item *protocol*.
– In the *Protocol number* field, enter the value `6`.
Specify a value according to the Assigned Internet Protocol Numbers defined by the IANA. Use this link to find a list of the protocol numbers:
https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
– Click the *Ok* button.

☐ Add the source IP address and mask to the class:

– Click the button.
The dialog displays the *Create* window.
– In the *Class name* field, enter the name `class1` or select it from the list.
– From the *Type* drop-down list, select the item *srcip*.
– In the *Source IP address* field, enter the value `10.20.10.11`.
– Click the *Ok* button.

☐ Add the source port to the class.

– Click the button.
The dialog displays the *Create* window.
– In the *Class name* field, enter the name `class1` or select it from the list.
– From the *Type* drop-down list, select the item *srcl4port*.
– In the *Source IP address* field, enter the value `80`.
– Click the *Ok* button.

☐ Apply the settings temporarily. To do this, click the button.

☐ Step 2: Add a policy.

☐ Open the *Switching* > *QoS/Priority* > *DiffServ* > *Policy* dialog.

☐ Create a policy:

– Click the button.
The dialog displays the *Create* window.
– In the *Policy name* field, enter the `policy1` item.
– From the *Direction* drop-down list, select the item *in*.
– In the *Class name* field, select the `class1` item.
– In the *Type* field, select the *drop* item.
– Click the *Ok* button.

☐ Apply the settings temporarily. To do this, click the button.

☐ Step 3: Assign the policy to a port.

- ☐ Open the *Switching > QoS/Priority > DiffServ > Assignment* dialog.
- ☐ Assign the policy to a port:
  - Click the button.
    The dialog displays the *Create* window.
  - From the *Port* drop-down list, select the port `1/1`.
  - From the *Direction* drop-down list, select the item *In*.
  - From the *Policy* drop-down list, select the item `policy1`.
  - Click the *Ok* button.

Note:
You cannot apply IP ACL rules and DiffServ rules together in the same direction on a port.

- ☐ Apply the settings temporarily. To do this, click the button.

☐ Step 4: Enable the function globally.

- ☐ Open the *Switching > QoS/Priority > DiffServ > Global* dialog.
- ☐ Enable the *DiffServ* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

When the link on the port is up, the value is `up`, in the *Status* column.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`class-map match-all class1`	To add a class named `class1`.
`class-map name class1 match protocol tcp`	To add the `tcp` protocol as a match condition to the class.
`class-map name class1 match srcip 10.20.10.11 255.255.255.0`	To add the source IP address `10.20.10.11` as a match condition to the class.
`class-map name class1 match srcl4port http`	To add the value `http` (TCP Port 80) as a match condition to the class.
`policy-map create policy1 in`	To add a policy named `policy1` for incoming data packets (`in`).
`policy-map name policy1 class add class1`	To assign the class with the name `class1` to the policy with the name `policy1`.
`policy-map name policy1 class name class1 drop`	To drop data packets.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`service-policy in policy1`	To assign the policy with the name `policy1` to the interface `1/1`.
`exit`	To change to the Configuration mode.
`diffserv enable`	To enable the *DiffServ* function globally.

10.6 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 superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to buffer overflow on a port. Shortly before the buffer memory of a port 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.

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 transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming data packets.

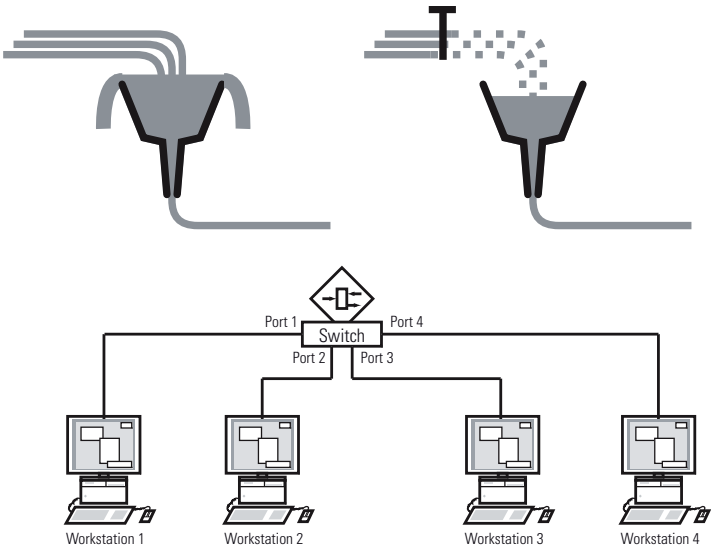


Figure 22: Example of flow control

10.6.1 Flow Control with a full-duplex link

In the example, there is a full-duplex 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.

10.6.2 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.
- ☐ Apply 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 reconfigure logical connections centrally than cable connections.

The device supports independent VLAN learning according to IEEE 802.1Q 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 the data packets 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 set up the VLANs.

11.1.1 Application example of a simple port-based VLAN

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.

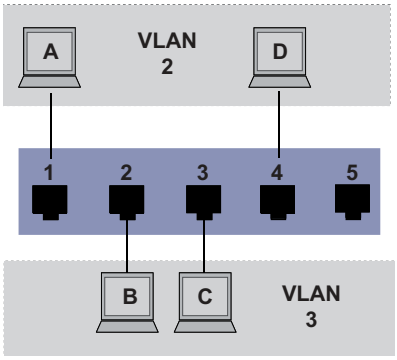


Figure 23: Example of a simple port-based VLAN

When setting up the VLANs, you add communication rules for every port, which you set up 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

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Table 23: Egress table

VLAN ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

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 add VLAN `3` with the name `VLAN3`.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN `2`.
`name 2 VLAN2`	To assign the name `2` to the VLAN `VLAN2`.
`vlan add 3`	To add VLAN `3`.
`name 3 VLAN3`	To assign the name `3` to the VLAN `VLAN3`.
`name 1 VLAN1`	To assign the name `1` to the VLAN `VLAN1`.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 512
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                          default    0 days, 00:00:05
2       VLAN2                          static     0 days, 02:44:29
3       VLAN3                          static     0 days, 02:52:26
```

☐ 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 the VLAN.
    Changes using the *GVRP* function are allowed.

  Because end devices usually interpret untagged data packets, you specify the value `U`.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ In the *Port-VLAN ID* column, specify 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 ports connected to an end device.
- ☐ Apply 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`vlan participation include 2`	The port 1/1 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID 2 to port 1/1.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface 1/2.
`vlan participation include 3`	The port 1/2 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID 3 to port 1/2.
`exit`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface 1/3.
`vlan participation include 3`	The port 1/3 becomes a member of the VLAN 3 and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID 3 to port 1/3.
`exit`	To change to the Configuration mode.
`interface 1/4`	To change to the Interface Configuration mode of interface 1/4.
`vlan participation include 2`	The port 1/4 becomes a member of the VLAN 2 and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID 2 to port 1/4.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.
`show vlan id 3`	To display details for VLAN 3.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

11.1.2 Application example of a complex VLAN setup

The second example displays a more complex configuration with 3 VLANs (1 to 3). Along with the Switch from example 1, you use a second Switch (on the right in the example).

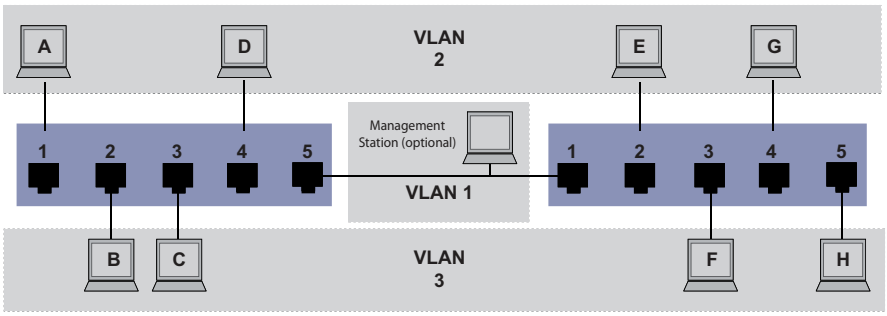


Figure 24: Example of a more complex VLAN configuration

The terminal devices (A to H) of the individual VLANs are spread over 2 transmission devices (Switches). Such VLANs are therefore known as distributed VLANs. An optional network management station is also shown, which has access to the device management of each network component if the associated VLAN is set up correctly.

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 both 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

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Table 25: Ingress table for device on right

Terminal	Port	Port VLAN identifier (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Table 26: Egress table for device on left

VLAN ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Table 27: Egress table for device on right

VLAN ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

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 specified above to adapt the previously set up 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, 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 add VLAN 3 with the name VLAN3.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 2`	To add VLAN 2.
`name 2 VLAN2`	To assign the name 2 to the VLAN VLAN2.
`vlan add 3`	To add VLAN 3.
`name 3 VLAN3`	To assign the name 3 to the VLAN VLAN3.
`name 1 VLAN1`	To assign the name 1 to the VLAN VLAN1.
`exit`	To change to the Privileged EXEC mode.
`show vlan brief`	To display the current VLAN configuration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 512
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

- 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 the 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.
- Apply the settings temporarily. To do this, click the button.
- Open the *Switching > VLAN > Port* dialog.
- In the *Port-VLAN ID* column, specify 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 ports connected to an end device.
- 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.
- Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`vlan participation include 1`	The port `1/1` becomes a member of the VLAN `1` and transmits the data packets without a VLAN tag.
`vlan participation include 2`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan tagging 2 enable`	The port `1/1` becomes a member of the VLAN `2` and transmits the data packets with a VLAN tag.
`vlan participation include 3`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan tagging 3 enable`	The port `1/1` becomes a member of the VLAN `3` and transmits the data packets with a VLAN tag.
`vlan pvid 1`	To assign the Port VLAN ID `1` to port `1/1`.
`vlan ingressfilter`	To activate ingress filtering on port `1/1`.
`vlan acceptframe vlanonly`	Port `1/1` only forwards packets with a VLAN tag.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`vlan participation include 2`	The port `1/2` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID `2` to port `1/2`.
`exit`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface `1/3`.
`vlan participation include 3`	The port `1/3` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.
`vlan pvid 3`	To assign the Port VLAN ID `3` to port `1/3`.
`exit`	To change to the Configuration mode.
`interface 1/4`	To change to the Interface Configuration mode of interface `1/4`.
`vlan participation include 2`	The port `1/4` becomes a member of the VLAN `2` and transmits the data packets without a VLAN tag.
`vlan pvid 2`	To assign the Port VLAN ID `2` to port `1/4`.
`exit`	To change to the Configuration mode.
`interface 1/5`	To change to the Interface Configuration mode of interface `1/5`.
`vlan participation include 3`	The port `1/5` becomes a member of the VLAN `3` and transmits the data packets without a VLAN tag.

```
vlan pvid 3                                          To assign the Port VLAN ID 3 to port 1/5.
exit                                                 To change to the Configuration mode.
exit                                                 To change to the Privileged EXEC mode.
show vlan id 3                                       To display details for VLAN 3.
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

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 responds 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 set up a Guest VLAN on a port 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 set up 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 set up 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 set-up Guest VLAN.

The following example explains how to add a Guest VLAN. Add 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.
- ☐ Enable the *802.1X* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply 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
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 10`	To add VLAN `10`.
`vlan add 20`	To add VLAN `20`.
`name 10 Guest`	To rename VLAN `10` to `Guest`.
`name 20 Unauth`	To rename VLAN `20` to `Unauth`.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dot1x system-auth-control enable`	To enable the *802.1X* function globally.
`dot1x port-control auto`	To enable port control on port `1/4`.
`interface 1/4`	To change to the Interface Configuration mode of interface `1/4`.
`dot1x guest-vlan 10`	To assign the guest vlan to port `1/4`.
`dot1x unauthenticated-vlan 20`	To assign the unauthorized vlan to port `1/4`.
`exit`	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 packets on a port, by VLAN and/or priority. A significant benefit of the voice VLAN is that a high volume of data on the port does not affect the sound quality of an IP phone.

The device uses the source MAC address to identify and prioritize the voice data flow. Identifying by MAC address reduces the potential for a "rogue client" to connect to the port and manipulate voice data packets.

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 packets with VLAN tag, priority tag 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 packets. The segregation of the data packets improves the quality of the voice data stream in case of high data volumes.

- Configuring the port to using 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.
- Specify 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 set up as *untagged*, the phone sends untagged packets.
- When set up as *none*, the phone uses its own configuration to send voice data packets.

11.5 MAC based VLANs

Use the MAC-based VLAN to forward the data packets based on the source MAC address associated with the VLAN. A MAC-based VLAN defines the filtering criteria for untagged or priority tagged packets.

You specify a MAC-based VLAN filter by assigning a specific source address to a MAC-based VLAN. The device forwards untagged packets received with the source MAC address on the MAC-based VLAN. The other untagged packets are subject to normal VLAN classification rules.

11.6 IP subnet-based VLANs

In an IP subnet-based VLAN, the device forwards the data packets based on the source IP address and subnet mask associated with the VLAN. User-defined filters determine if a packet belongs to a particular VLAN.

Use the IP subnet-based VLAN to specify the filtering criteria for untagged or priority tagged packets. For example, assign a specific subnet address to an IP subnet-based VLAN. When the device receives untagged packets from the subnet address, it forwards them to the IP subnet-based VLAN. Other untagged packets are subject to normal VLAN classification rules.

To set up an IP subnet-based VLAN, specify an IP address, a subnet mask and the associated VLAN ID. In case of multiple matching entries, the device associates the VLAN ID to the entry with the longer prefix first.

11.7 Protocol-based VLAN

In a protocol-based VLAN, the device bridges the data packets through specified ports based on the protocol associated with the VLAN. User-defined packet filters determine if a packet belongs to a particular VLAN.

Set up protocol-based VLANs using the value in the *Ethertype* column as the filtering criteria for untagged packets. For example, assign a specific protocol to a protocol-based VLAN. When the device receives untagged packets with the protocol, it forwards them to the protocol-based VLAN. The device assigns the other untagged packets to the port VLAN ID.

11.8 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. According to IEEE 802.1Q, the function governs how the device processes VLAN tagged packets.

Use the VLAN aware mode to apply the user-defined VLAN topology set up by the network administrator. When the device forwards packets, it uses VLAN tagging and 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 the data packets 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 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

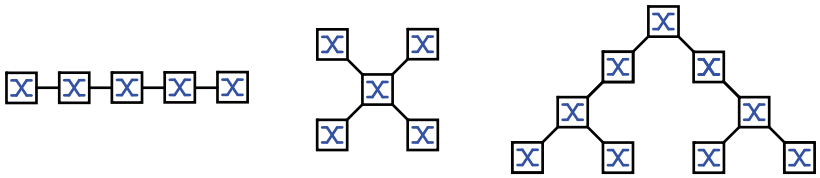


Figure 25: Network with line, star and tree topologies

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 looping. The result is a meshed topology.

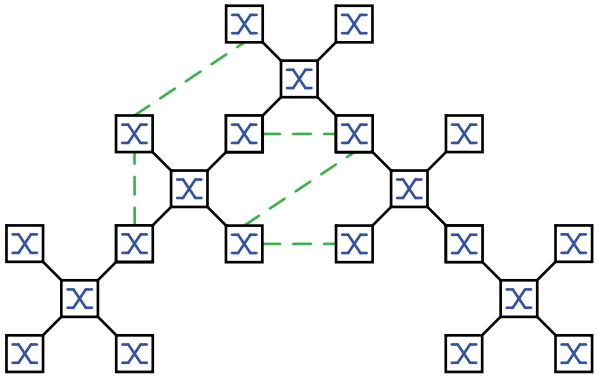


Figure 26: Meshed topology: Tree topology with physical loops

For operating in this network topology, the device provides you with the following redundancy protocols:

- Rapid Spanning Tree Protocol (RSTP)

Ring topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This results in a ring topology.

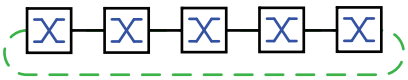


Figure 27: Ring topology: Line topology with connected ends

For operating in this network topology, the device provides you with the following redundancy protocols:

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree Protocol (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

Redundancy protocol	Network topology	Comments
MRP	Ring	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 Media Redundancy Protocol (MRP) according to IEC 62439. When you only use Hirschmann devices, up to 100 devices are possible in the MRP Ring.
Sub Ring	Ring	The *Sub Ring* function lets you easily couple network segments to existing redundancy rings.
Ring/Network coupling	Ring	
RCP	Ring	
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 the data packets to the backup link. You typically use Link Backup in service-provider or enterprise networks.
HIPER Ring Client	Ring	Extend an existing HIPER Ring or replace a device already participating as a client in a HIPER Ring.
HIPER Ring over LAG	Ring	Link devices together over a Link Aggregation Group (LAG). The *Ring Manager* and *Ring Client* devices behave in the same manner as a ring without a LAG instance.

Note:
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.

12.1.3 Combinations of redundancy protocols

Table 29: Overview of redundancy protocol combinations

	MRP	RSTP/MSTP	Link Aggreg.	Link Backup	Sub Ring	HIPER Ring
MRP	▲	—	—	—	—	—
RSTP/ MSTP [3]	▲[1]	▲	—	—	—	—
Link Aggreg.	▲2)	▲[2]	▲	—	—	—

Table 29: Overview of redundancy protocol combinations (cont.)

	MRP	RSTP/MSTP	Link Aggreg.	Link Backup	Sub Ring	HIPER Ring
Link Backup	▲	▲	▲	▲	—	—
Sub Ring	▲	▲	▲ 2)	▲	▲	—
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Combination applicable

○ Combination not applicable

1) A redundant coupling between these network topologies will possibly lead to loops. To redundantly couple these topologies, refer to chapter “FuseNet function” on page 253.

2) Combination applicable on the same port

3) In combination with MSTP, the failover times of other redundancy protocols can slightly increase.

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 Media Redundancy Protocol (MRP) 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 the *Ring Manager* device detects a primary ring link failure, it 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.

Using the *Ring manager* function, the two ends of a backbone in a line structure can be closed to a redundant ring. The *Ring Manager* device keeps the redundant line open as long as the line structure is intact. When a segment becomes inoperable, the *Ring Manager* device immediately closes the redundant line, and line structure is intact again.

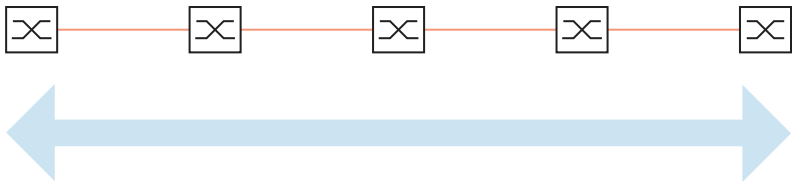


Figure 28: Line structure

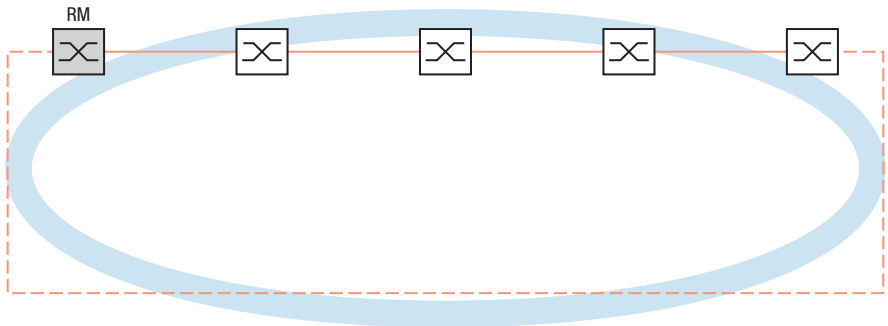


Figure 29: Redundant ring structure
RM = Ring Manager
—— main line
- - - redundant line

12.2.2 Reconfiguration time

When a line section failure is detected, the *Ring Manager* device changes the MRP Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the *Ring Manager* device.

Possible values for the maximum delay time:
- `500ms`
- `30ms`

Note:
If every device in the ring supports the shorter delay time, then you can set up 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 time, the device provides the *Advanced mode*. When the ring participants inform the *Ring Manager* device about interruptions in the ring through *Link Down* notifications, the *Advanced mode* speeds up the link failure detection.

Hirschmann devices support *Link Down* notifications. Therefore, you generally activate the *Advanced mode* in the *Ring Manager* device.

When you are using devices that do not support *Link Down* notifications, the *Ring Manager* device 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* device.
- There is exactly one *Ring Manager* device in the ring.

If you are using VLANs, then set up 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

The Media Redundancy Protocol (MRP) uses *Test*, *Link Change*, and *Topology Change* (*FDB Flush*) packets.

The *Ring Manager* device is connected to the ring with 2 ring ports. As long as all connections in the ring are operational, the *Ring Manager* device 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 *Ring Manager* device prevents a network loop.

The *Ring Manager* device periodically sends test packets into the ring from both ring ports. The test packets are special packets. The *Ring Manager* device sends and receives test packets even at the redundant port although the redundant port blocks normal packets. The *Ring Manager* device expects to receive the test packets on its respective other ring port. If the *Ring Manager* device does not receive any expected test packets for a specified amount of time, it detects a ring failure.

If the *Advanced mode* function is active, the *Ring Manager* device also reacts to *Link Down* packets. The prerequisite is that each device in the ring can send a *Link Change* packet when the link to the next device in the ring changes. These packets help the *Ring Manager* device react more quickly to a link failure or recovery. The *Ring Manager* device receives the *Link Change* packets even on its redundant port.

On reconfiguration of the ring, the *Ring Manager* device flushes its MAC address table (forwarding database) and sends *Topology Change* packets to the devices participating in the ring. The *Topology Change* packets prompt the other devices participating in the ring to flush their MAC address table (forwarding database), too. This procedure helps forward the payload packets over the new path more quickly. This procedure applies regardless of whether the ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

Table 30: MRP Packets

Packet Type	Send Mode	Time Parameter	Value
Test packet[1]	Periodically	Send interval	50 ms (for ring recovery time 500 ms) 20 ms (for ring recovery time 200 ms)
		Reception timeout	400 ms (for ring recovery time 500 ms) 160 ms (for ring recovery time 200 ms)
Link Down packet[2]	Event-driven	On link-down of a ring port	-
Topology Change packet[3]	Event-driven	On reconfiguration	-

1. Sent by the *Ring Manager* device only.
2. Sent by supporting ring participants.
3. The reception of a *Topology Change* packet prompts the supporting devices participating in the ring to flush their MAC address table (forwarding database).

MRP Packet Prioritization

The devices participating in the ring send *Test*, *Link Change*, and *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 forward and send 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 *Ring Client* devices:

- ☐ Specify the MRP VLAN ID to a value ≥1.
- ☐ Specify the ring ports as T (tagged) members of this MRP VLAN.

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. If the MRP VLAN does not yet exist, the device automatically sets up 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 Application example of an MRP Ring

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* device sends data on the secondary ring link. When the primary link is restored, the secondary link reverts back to the backup mode.

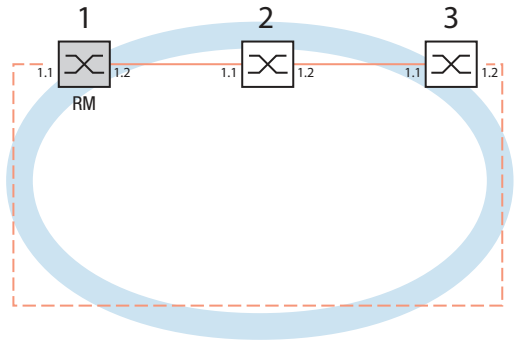


Figure 30: Example of MRP Ring
RM = Ring Manager
—— main line
- - - redundant line

The following example configuration describes the configuration of the *Ring Manager* device (1). You set up 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 `30ms` as the ring recovery time. Every device supports the *Advanced mode* function.

- ☐ Set up the network to meet your demands.
- ☐ To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up *100M FDX*.
  - For the other port types, keep the port-specific default settings.

Note:
Set up 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`no spanning-tree operation`	To switch Spanning Tree off.
`show spanning-tree global`	To display the parameters for checking.

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. Set up 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 add an MRP domain with the ID `default-domain`.
`mrp domain modify port primary 1/1`	To specify port `1/1` as *primary* ring port.
`mrp domain modify port secondary 1/2`	To specify port `1/2` as the *secondary* ring port.

Enable the *Fixed backup* port. To do this, perform the following steps:

- ☐ Enable the *Ring manager* function.
  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* device 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* function.
  For the other devices in the ring, leave the setting as *Off*.

```
mrp domain modify mode   manager
```

To designate the device as the *Ring Manager* device. 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 the network, then select the value *500ms*.

- ☐ Switch the operation of the MRP Ring on.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
mrp domain modify operation   enable
```

To activate the MRP Ring.

When every ring participant is set up, close the line to create 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 operates in the *Ring Client* or *Ring Manager* mode, the following messages are possible:
- *Redundancy available. Ring is closed.*
  The redundancy is set up. When a component of the ring is inoperable, the redundant line takes over its function.
- *Configuration error: Error on ring port link.*
  An error is detected in the cabling of the ring ports.

When the device operates in the *Ring Manager* mode, the following messages are possible:
- *Configuration error: Packets from another ring manager received.*
  Another device exists in the ring that operates in the *Ring Manager* mode.
  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 set-up VLANs the device transmits the MRP packets.
To set the MRP VLAN ID, first set up 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 let you 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 connections into one logical connection between 2 devices. The parallel links increase the bandwidth between the 2 devices.

An MRP Ring consists of up to 50 devices that support the Media Redundancy Protocol (MRP) according to IEC 62439. When you use only Hirschmann devices, the protocol lets you set up 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* device monitors both ends of the backbone for continuity. The *Ring Manager* device blocks data on the secondary (redundant) port as long as the backbone is intact. When the *Ring Manager* device 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.

For the *Ring Manager* device 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 set up a LAG instance on individual 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 the 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.

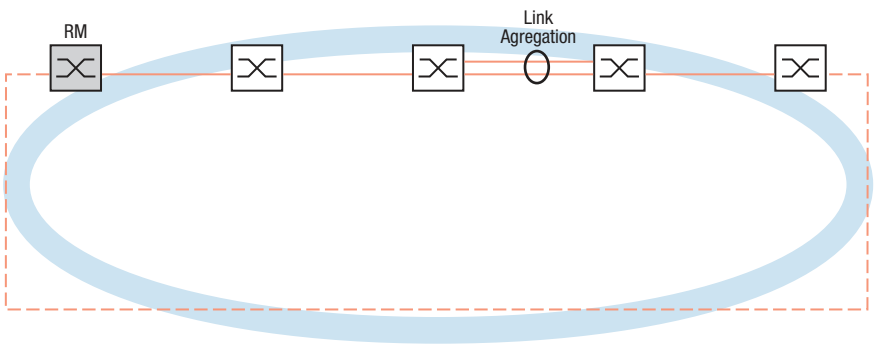


Figure 31: Link Aggregation over a single link of an MRP Ring.

LAG on an entire MRP Ring

Besides being able to set up a LAG instance on specific segments of an MRP Ring, Hirschmann devices also allow you to set up LAG instances on every segment, which increases bandwidth on the entire MRP Ring.

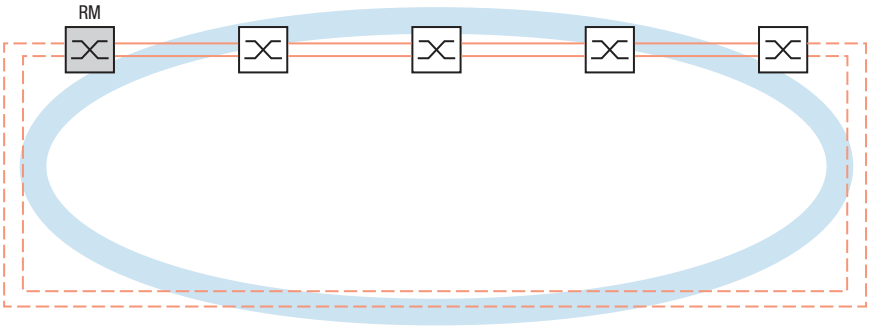


Figure 32: Link Aggregation over the entire MRP Ring.

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 *Ring Manager* device detects that the ring is open and begins forwarding data on the secondary port. This way the *Ring Manager* device is able to restore continuity to the devices on the other side of the interrupted segment.

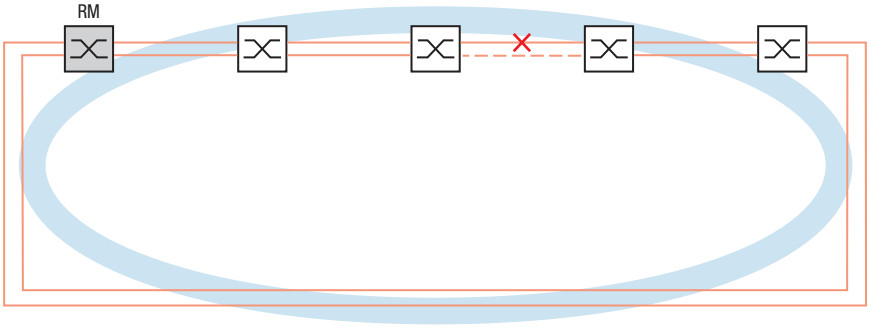


Figure 33: Interruption of a link in an MRP Ring

Application example for MRP over LAG

In the following example, switch A and switch B link two departments. The data volume of the departments exceeds the individual bandwidth capacity of the ports. You set up an 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.

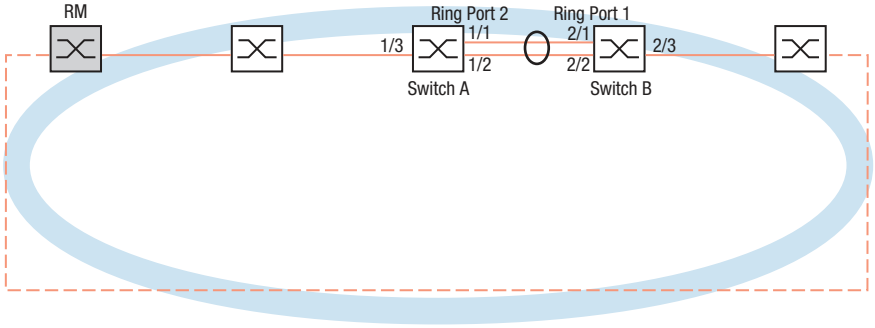


Figure 34: Application example of an MRP over LAG setup

Set up switch A first. To do this, perform the following steps. Then set up switch B using the same steps, substituting the appropriate port and ring port numbers.

- ☐ Open the *Switching > L2-Redundancy > Link Aggregation* dialog.
- ☐ Click the 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.
- ☐ 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* device detects 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.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ In the *Ring port 2* frame, select port `lag/1` from the *Port* drop-down list.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	To add port `1/1` to the Link Aggregation Group `lag/1` .

`link-aggregation modify lag/1 addport 1/2`	To add port `1/2` to the Link Aggregation Group `lag/1` .
`mrp domain modify port secondary lag/1`	To specify port `lag/1` as *secondary* ring port.
`copy config running-config nvm`	To save the current settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

12.3 HIPER Ring Client

The concept of HIPER Ring Redundancy enables the construction of high-availability, ring-shaped network structures. The *HIPER Ring* Client function lets the network administrator extend an existing HIPER Ring or replace a client device already participating in a HIPER Ring.

When the device senses that the link on a ring port becomes inoperable, the device sends a *Link Down* packet to the *Ring Manager* device and flushes the MAC address table (forwarding database). As soon as the *Ring Manager* device receives the *Link Down* packet, it immediately forwards the data stream over both the primary and secondary ring ports. Thus, the *Ring Manager* device is able to maintain the integrity of the HIPER Ring.

The device only supports Fast Ethernet and Gigabit Ethernet ports as ring ports. Furthermore, you can include the ring ports in a LAG instance.

In the default state, the *HIPER Ring Client* mode is inactive, and the primary and secondary ports are not set up.

To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:

- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify *100M FDX*.
- For the other port types, keep the port-specific default settings.

Note:
Deactivate in the *Switching > L2-Redundancy > Spanning Tree > Port* dialog the *Spanning Tree* function for the ring ports. STP and HIPER Ring have different reaction times.

12.3.1 VLANS on the HIPER Ring

The device lets you forward VLAN data over the HIPER Ring. Thus, the device provides redundancy for your VLAN data. The device forwards management data around the ring, for example, on VLAN 1. For the data to reach the management station, the devices participating in the ring forward the untagged management data to their ring ports. Also, specify the ring ports as members of VLAN 1.

When you have other VLANs traversing your ring, the devices participating in the ring forward the other VLAN data as tagged.

Specify the VLAN settings. To do this, perform the following steps on the *Ring Manager* and *Ring Client* devices:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Forward untagged VLAN management data on the ring ports.
  For VLAN 1, select in the columns related to the ring ports the `U` item from the drop-down list.
- ☐ Block redundancy protocol packets from being forwarded to the non-ring ports:
  For VLAN 1, select in the columns **not** related to the ring ports the `-` item from the drop-down list.

- Allow a device participating in the ring to forward VLAN data to and from ports with VLAN membership.
  For the other VLANs, select in the columns related to the ring ports the `T` item from the drop-down list.
- Open the *Switching > VLAN > Port* dialog.
- Assign VLAN 1 membership to the ring ports.
  Enter the value `1` in the *Port-VLAN ID* column of the ring port rows.
- Assign VLAN membership to the non-ring ports.
  Enter the appropriate VLAN ID in the *Port-VLAN ID* column of the non-ring port rows.

12.3.2 Advanced Information

The HIPER Ring is the proprietary predecessor of MRP. The HIPER Ring works similar to MRP but uses different packets. For setting up a new redundant ring, Hirschmann recommends using MRP.

HIPER Ring Packets

The HIPER Ring protocol uses *Test*, *Link Down*, and *Topology Change* packets.

Note:
HiOS devices offer *HIPER Ring Client* functions. The *HIPER Ring Manager* functions are offered by devices with Classic Software. The *HIPER Ring Manager* functions are mentioned here only for completeness. For details, refer to the documentation of your HIPER Ring Manager device.

The *Ring Manager (RM)* device is connected to the ring with 2 ring ports. As long as all connections in the ring are operational, the *Ring Manager* device 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 *Ring Manager* device prevents a network loop.

The *Ring Manager* device periodically sends test packets into the ring from both ring ports. The test packets are special packets. The *Ring Manager* device sends and receives test packets even at the redundant port although the redundant port blocks normal packets. The *Ring Manager* device expects to receive the test packets on its respective other ring port. If the *Ring Manager* device does not receive any expected test packets for a specified amount of time, it detects a ring failure.

When a link between 2 devices participating in the ring becomes inoperable, the affected devices send a *Link Down* packet to the *Ring Manager* device. This helps the *Ring Manager* device react more quickly to a link failure. The *Ring Manager* device receives the *Link Down* packets even on its redundant port.

On reconfiguration of the ring, the *Ring Manager* device flushes its MAC address table (forwarding database) and sends *Topology Change* packets to the devices participating in the ring. The *Topology Change* packets prompt the other devices participating in the ring to flush their MAC address table (forwarding database), too. This procedure helps forward the payload packets over the new path more quickly. This procedure applies regardless of whether the ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

Table 31: HIPER Ring Packets

Packet Type	Send Mode	Time Parameter	Value
Test packet[1]	Periodically	Send interval[2]	20 ms (Ring recovery time accelerated) 60 ms (Ring recovery time standard)
		Reception timeout	280 ms (Ring recovery time accelerated) 480 ms (Ring recovery time standard)
Link Down packet[3]	Event-driven	On link-down of a ring port	-
Topology Change packet[4]	Event-driven	On reconfiguration	-

1. Sent by the *HIPER Ring Manager* device (Classic Software) only.
2. Specified in the *HIPER Ring Manager* device (Classic Software) only.
3. Sent by supporting ring participants.
4. The reception of a *Topology Change* packet prompts the supporting devices participating in the ring to flush their MAC address table (forwarding database).

HIPER Ring Packet Prioritization

The devices participating in the ring send *Test*, *Link Change*, and *Topology Change* packets with the fixed VLAN ID 1. In the default setting, these packets are 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 *Ring Manager* and *Ring Client* devices then forward and send these packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To do that, specify on the *Ring Manager* device (Classic software) and *Ring Client* devices the ring ports as T (tagged) members of VLAN 1.

Note:
These settings for VLAN 1 are different from the VLAN settings described in chapter “VLANS on the HIPER Ring” on page 226.

12.3.3 HIPER Ring over LAG

The *HIPER Ring* function lets you link the devices together over a Link Aggregation Group (LAG). The *Ring Manager* and *Ring Client* devices behave in the same manner as a ring without a LAG instance.

If an LAG link goes down, then the other link in the instance also goes down making a break in the ring. After detecting a break in the ring, the affected ports send a *Link Down* packet to the *Ring Manager* device. The *Ring Manager* device unblocks its redundant port, sends data in both directions in the ring, and replies with a *Topology Change* packet. Upon receiving a *Topology Change* packet, the ring participants flush their MAC address table (forwarding database).

12.4 Spanning Tree

Note:
The Spanning Tree Protocol (STP) 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 subnets can lead to loops and thus interruption of communication across the network. 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).

12.4.1 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.
- The topology stabilizes within a predictable time period.
- The administrator can specify and reproduce the topology.
- Transparency for the end devices.
- The network load is low relative to the available transmission capacity due to the tree structure set-up.

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* of the bridge ports
- *Port Identifier*

Bridge Identifier

The *Bridge Identifier* consists of 8 bytes. The bridge with the numerically lowest *Bridge Identifier* value has the highest 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 `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 result, the bridge administrator can set the *Bridge priority* in steps of 4096. The default value is `32768` (8000H), and the max. value is `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*.

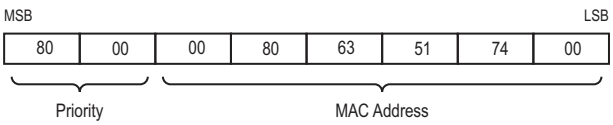


Figure 35: Bridge Identifier, Example (interpretation according to IEEE 802.1D-1998, values in hexadecimal notation)

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 32 on page 231). The device assigns a higher path cost to paths with lower transmission speeds.

As an alternative, 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 path costs from the port of the connected bridge to the *Root bridge*.

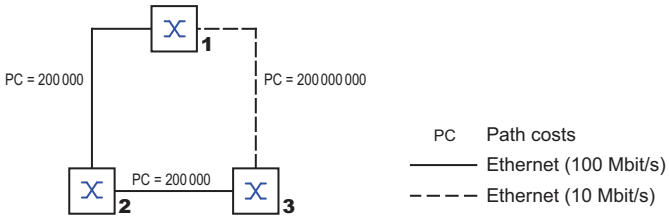


Figure 36: Path costs

Table 32: Recommended path costs for RSTP based on the data rate.

Data rate	Recommended value	Recommended range	Possible range
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 Tbit/s	20	2-200	1-200000000
10 Tbit/s	2	1-20	1-200000000

1. Verify that bridges, which conform to IEEE 802.1D-1998 and only support 16-bit values for the past 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 result, 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).

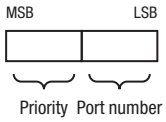


Figure 37: Port Identifier (interpretation according to IEEE 802.1D-1998)

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.

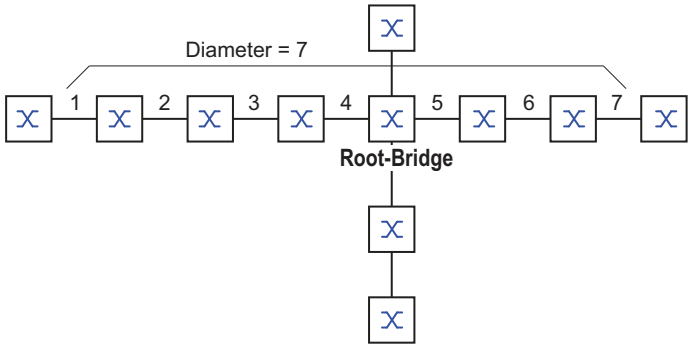


Figure 38: Definition of diameter

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 is 19. When you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved is 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.

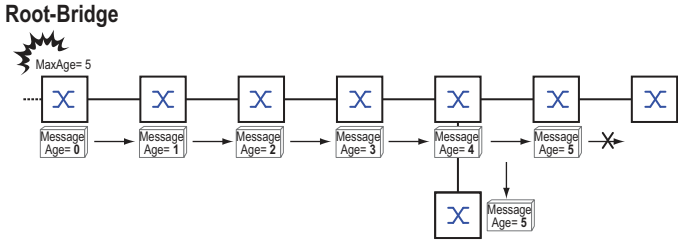


Figure 39: Transmission of an STP-BPDU depending on MaxAge

12.4.2 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 cost*
- *Port Identifier*

(see IEEE 802.1D)

Setting up the tree structure

The bridge with the numerically lowest *Bridge Identifier* value is called the *Root bridge*. This bridge 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, the bridge further from the root uses the *Bridge Identifiers* of the bridge closer to the root. The the bridge further from the root 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 232). 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.

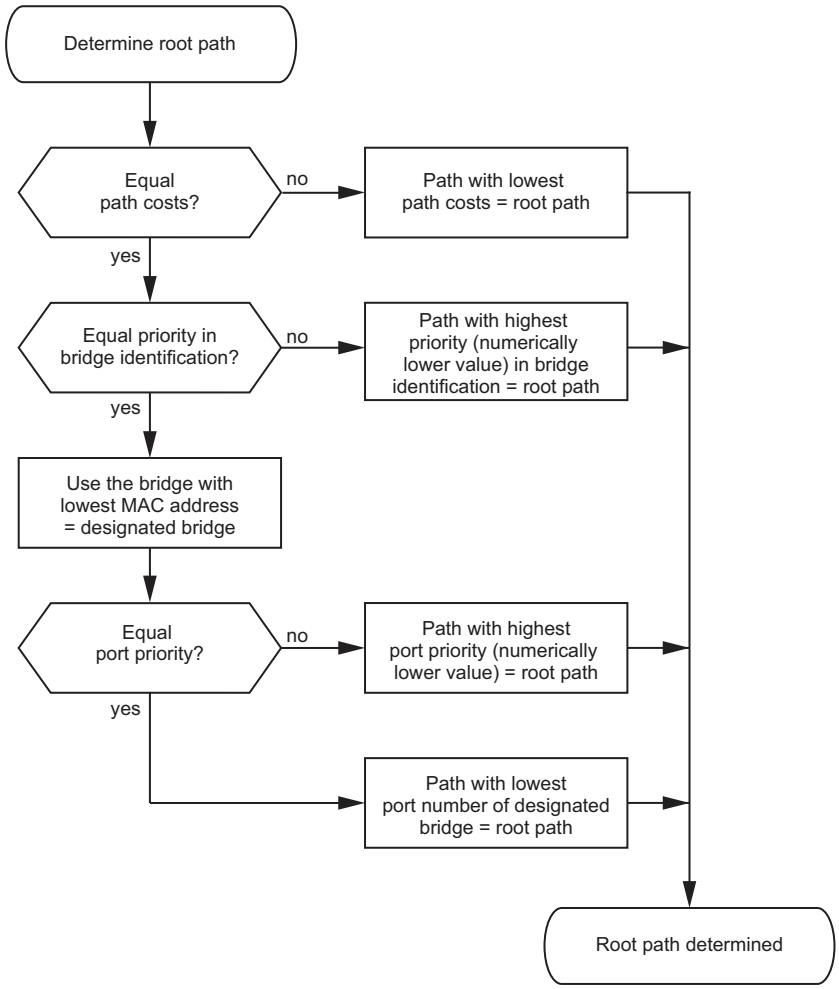


Figure 40: Flow diagram for specifying the root path

12.4.3 Examples

Example of determining the root path

You can use the network plan to follow the flow chart (see figure 40 on page 234) for determining the root path. The administrator has specified a priority in the *Bridge Identifier* for each bridge. The bridge with the numerically lowest value for the *Bridge Identifier* 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 has 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 Identifier* (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).

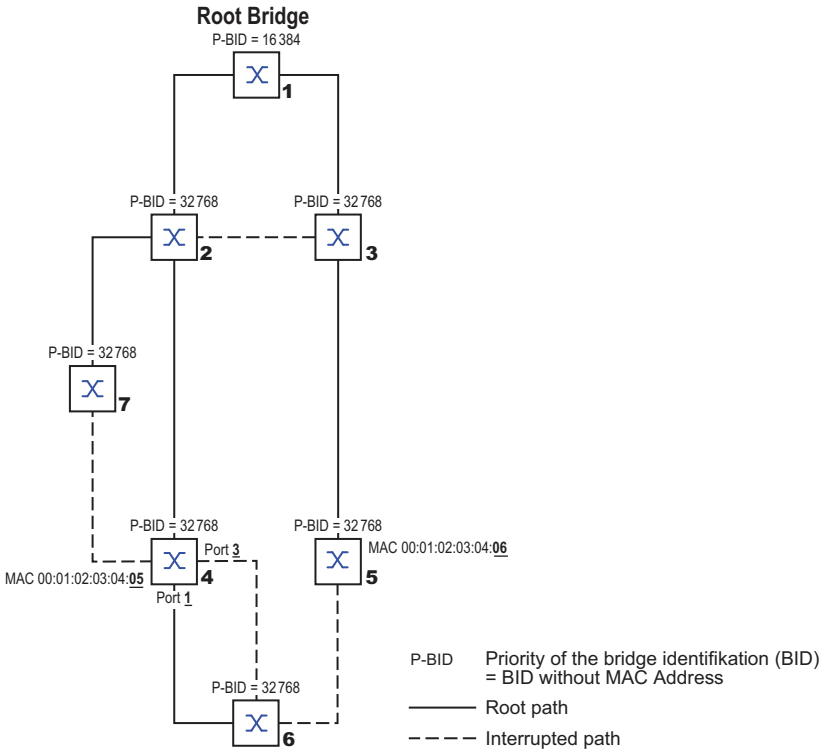


Figure 41: Example of a network plan for determining the root path

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 234) 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 lower than the value 32768.

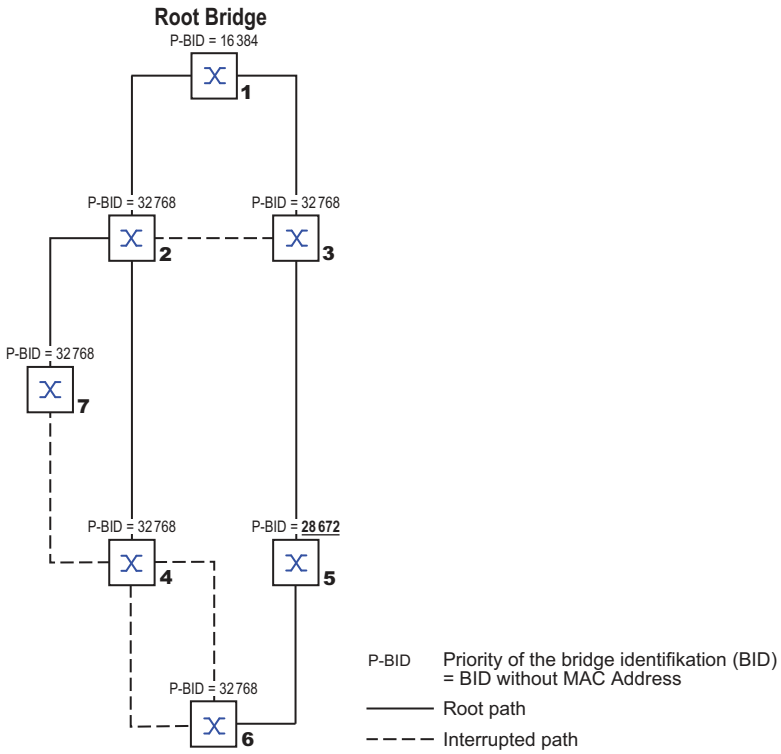


Figure 42: Example of a network plan for manipulating the root path

Example of manipulating the tree structure

The 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 administrator sets up bridge 2 as the *Root bridge*, the burden of the control packets on the subnets 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.

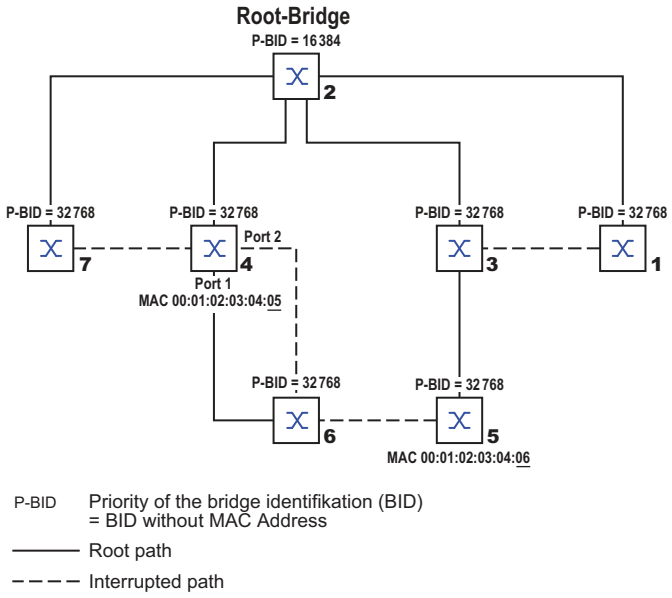


Figure 43: Example of manipulating the tree structure

12.5 Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP) uses the same algorithm for determining the tree structure as Spanning Tree Protocol (STP). When a link or bridge becomes inoperable, the Rapid Spanning Tree Protocol (RSTP) adds mechanisms that speed up the reconfiguration.

The ports play a significant role in this context.

12.5.1 Port roles

The Rapid Spanning Tree Protocol (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 Identifier* 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 234.
  The *Root bridge* itself does not have a *Root port*, only *Designated ports*.
- *Designated port*:
  The bridge in a network segment that has the numerically lowest *Root path costs* value is the *Designated bridge*.
  When more than one bridge has the same *Root path costs*, the bridge with the numerically lowest *Bridge Identifier* value 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 through 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.

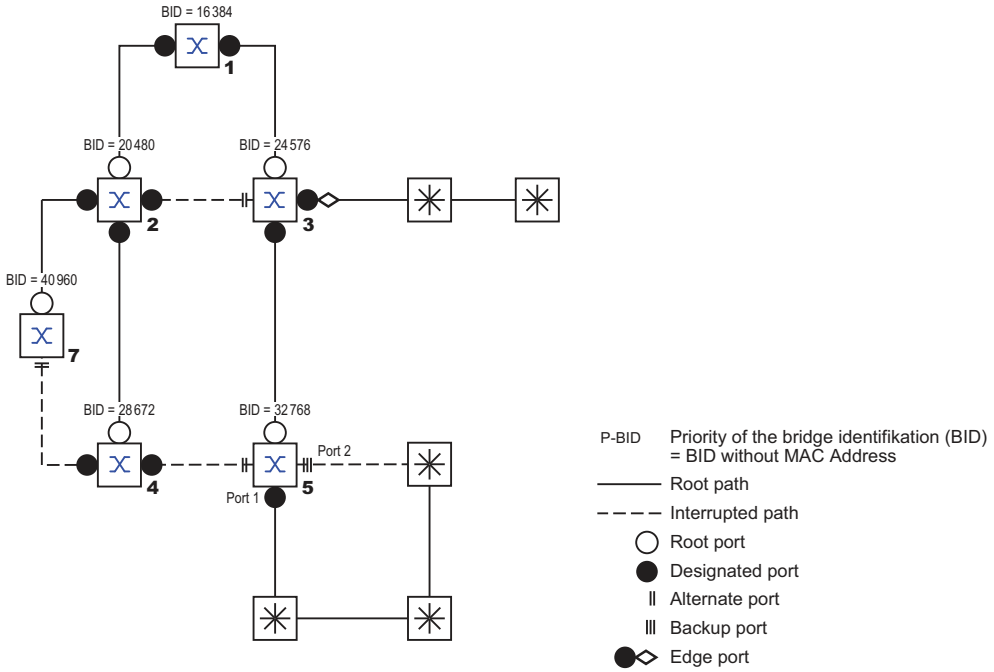


Figure 44: Port role assignment

12.5.2 Port states

Depending on the tree structure and the state of the selected connection paths, RSTP assigns the ports their states.

Table 33: Relationship between port state values for STP and RSTP

STP port state	Administrative bridge port state	MAC Operational	RSTP Port state	Active topology (port role)
Disabled	Disabled	FALSE	*Discarding*[1]	Excluded (disabled)
Disabled	Enabled	FALSE	*Discarding*[a]	Excluded (disabled)
Blocking	Enabled	TRUE	*Discarding*[2]	Excluded (alternate, backup)
Listening	Enabled	TRUE	*Discarding*[b]	Included (root, designated)
Learning	Enabled	TRUE	*Learning*	Included (root, designated)
Forwarding	Enabled	TRUE	*Forwarding*	Included (root, designated)

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 the MAC address table (forwarding database), no data packets except for STP-BPDUs

- *Learning*: Address learning active in the MAC address table (forwarding database), no data packets apart from STP-BPDUs
- *Forwarding*: Address learning in the MAC address table (forwarding database) active, sending and receiving of every packet type (not only STP-BPDUs)

12.5.3 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 BPDUs* and contains the following information:

- *Bridge Identifier* of the *Root bridge*
- *Root path costs* of the sending bridge
- *Bridge Identifier* of the sending bridge
- *Port Identifier* of the port through which the message was sent
- *Port Identifier* of the port 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.

12.5.4 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 Spanning Tree Protocol (STP), the age of the entries in the MAC address table (forwarding database) determines the updating of communication. The Rapid Spanning Tree Protocol (RSTP) immediately deletes the entries in those ports affected by a reconfiguration.
- Reaction to events:
  Without having to match any time specifications, Rapid Spanning Tree Protocol (RSTP) immediately reacts to events, for example, connection interruption and connection reinstatement.

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 (STP) or select another redundancy procedure described in this manual.

12.5.5 Configuring the device

RSTP sets up the network topology completely autonomously. The device with the numerically lowest *Bridge priority* value 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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`spanning-tree operation`	To enable Spanning Tree.
`show spanning-tree global`	To display the parameters for checking.

Now connect the redundant lines.

Define the settings for the device that takes over the role of the *Root bridge*.

Perform the following steps:

- ☐ In the *Priority* field you specify a numerically lower value.
  The bridge with the numerically lowest *Bridge Identifier* value has the highest priority and becomes the *Root bridge* of the network.
- ☐ Apply the settings temporarily. To do this, click the button.

`spanning-tree mst priority 0 <0..61440>`	To specify the *Bridge priority* of the device.

Note:
Specify the *Bridge priority* in the range `0..61440` in steps of 4096.

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`.

`show spanning-tree global`	To display the parameters for checking.

- ☐ 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.
- ☐ Apply 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.

Note:
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.

Note:
When possible, do not change the value in the “Hello Time” field.

Check the following values in the other devices:
- *Bridge Identifier* (*Bridge priority* and MAC address) of the corresponding device and the *Root bridge*.
- Number of the port that leads to the *Root bridge*.
- Path cost from the *Root port* of the device to the *Root bridge*.

Perform the following steps:

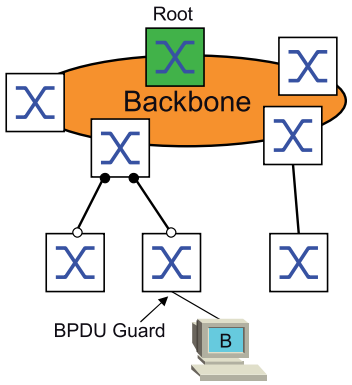
`show spanning-tree global`	To display the parameters for checking.

12.5.6 Guards

The device lets you activate various protection functions (guards) on the ports.

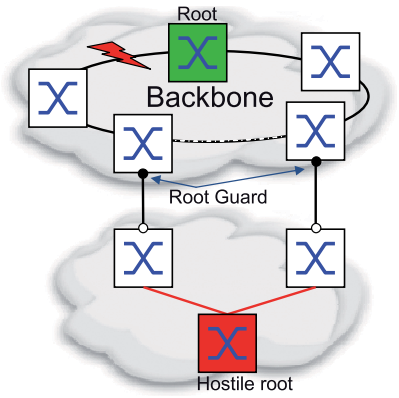
The following protection functions help protect the network from incorrect configurations, loops and attacks with STP-BPDUs:

- *BPDU guard* – for manually specified *Edge ports* (ports connected to an end device)
  You activate this protection function globally in the device.



  Ports connected to an end device 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 port.

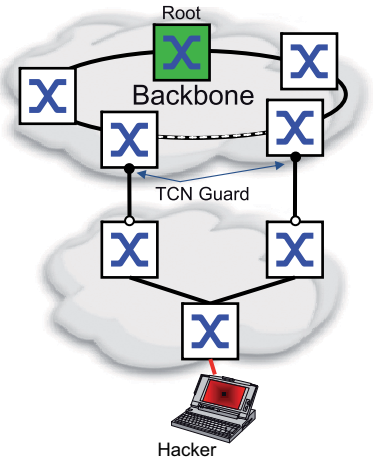
- *Root guard* – for *Designated ports*
  You activate this protection function separately for every port.



  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`.

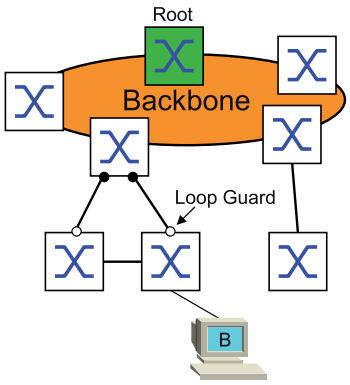
  When there are no STP-BPDUs with better path information to the *Root bridge*, after 2 × *Hello time [s]* the device resets the state of the port to a value according to the port role.

- *TCN guard* – for ports that receive STP-BPDUs with a *Topology Change* flag
  You activate this protection function separately for every 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 MAC address table (forwarding database) of the port. However, additional information in the BPDU that changes the topology is processed by the device.

- *Loop guard* – for *Root ports*, *Alternate ports* and *Backup ports*
  You activate this protection function separately for every 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 function

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ Mark the *BPDU guard* checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable` To change to the Privileged EXEC mode.

`configure`	To change to the Configuration mode.
`spanning-tree bpdu-guard`	To activate the *BPDU guard* function.
`show spanning-tree global`	To display the parameters for checking.

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.
- ☐ Switch to the *CIST* tab.
- ☐ For the ports connected to an end device, mark the checkbox in the *Admin edge port*column.
- ☐ Apply the settings temporarily. To do this, click the  button.

`interface <slot/port>`	To change to the Interface Configuration mode of interface `<x/y>`.
`spanning-tree edge-port`	To designate the port as an *Edge port* (port connected to an end device).
`show spanning-tree port <slot/port>`	To display the parameters for checking.
`exit`	To leave the interface 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:

In the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *Guards* tab, the checkbox in the *BPDU guard effect* column is marked.

`show spanning-tree port <slot/port>`	To display the parameters of the port for checking. The value of the *BPDU guard effect* parameter is `enabled`.

Reset the status of the 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* (port connected to an end device).
    or
  - – Deactivate the *BPDU guard* function.
- ☐ Activate the port again.

Activating the Root guard / TCN guard / Loop guard function

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 ports*, *Alternate ports* 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.

- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface <slot/port>`	To change to the Interface Configuration mode of interface `<x/y>`.
`spanning-tree guard-root`	To activate the *Root guard* function on the *Designated port*.
`spanning-tree guard-tcn`	To activate the *TCN guard* function on the port that receives STP-BPDUs with a *Topology Change* flag.
`spanning-tree guard-loop`	To activate the *Loop guard* function on a *Root port*, *Alternate port*, or *Backup port*.
`exit`	To leave the interface mode.
`show spanning-tree port <slot/port>`	To display the parameters of the port for checking.

12.5.7 Ring only mode function

You use the *Ring only mode* function to recognize full-duplex connectivity and to set up the ports that are connected to the end stations. The *Ring only mode* function lets the device transition to the *forwarding* state, and suppress the *Topology Change Notification* PDUs.

Configuring the Ring only mode

When you activate the *Ring only mode* function on the ports, and the device ignores the message age of normal BDPUs, the device sends *Topology Change* messages with the message age of 1.

Setting up the Ring only mode function

The given example describes the configuration of the *Ring only mode* function.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- ☐ In the *Ring only mode* frame, select the port `1/1` in the *First port* field.
- ☐ In the *Ring only mode* frame, select the port `1/2` in the *Second port* field.
- ☐ To activate the function, in the *Ring only mode* frame, mark the *Active* checkbox.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`spanning-tree ring-only-mode operation`	To enable the *Ring only mode* function.
`spanning-tree ring-only-mode first-port 1/1`	To specify port `1/1` as the first interface.
`spanning-tree ring-only-mode second-port 1/2`	To specify port `1/2` as the second interface.

12.6 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 connections into one logical connection between 2 devices. The parallel links increase the bandwidth 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 set up in parallel, the other links in the group continue to forward the data packets.

The device uses a hash option to determine load balancing across the port group. Tagging the egress data packets lets the device transmit associated packets across the same link.

The default settings for a new *Link Aggregation* instance are as follows:
- In the *Configuration* frame, the value in the *Hashing option* field is `sourceDestMacVlan`.
- 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 *Hashing option* column, the value is `sourceDestMacVlan`.
- In the *Active ports (min.)* column, the value is `1`.

12.6.1 Methods of Operation

The device operates on the Single Switch method. The Single Switch method provides you an inexpensive way to grow the 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 network load across the group member ports.

The device also uses the Same Link Speed method in which the group member ports operate in 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 a maximum of 16 Link Aggregation groups.

Hash Algorithm

The frame distributor is responsible for receiving frames from the end devices and transmitting them over the Link Aggregation Group. The frame distributor implements a distribution algorithm responsible for choosing the link used for transmitting any given packet. The hash option helps you achieve load balancing across the group.

The following list contains options which you set for link selection.
- Source MAC address, VLAN ID, EtherType, and receiving port
- Destination MAC address, VLAN ID, EtherType, and receiving port
- Source/Destination MAC address, VLAN ID, EtherType, and receiving port

- Source IP address and Source TCP/UDP port
- Destination IP address and destination TCP/UDP port
- Source/destination IP address and source/destination TCP/UDP port

Static and Dynamic Links

The device lets you set up static and dynamic links.

- Static Links
  The administrator sets up and maintains the links manually. For example, when a link fails and there is a media converter between the devices, the media converter continues forwarding the data packets on the link, causing the link to fail. Another possibility is that cabling or an undetected configuration mistake causes undesirable network behavior. In this case, the network administrator manually changes the link setup to restore the data stream.
- Dynamic Links
  The device confirms that the setup on the remote device is able to handle link aggregation and failover occurs automatically.

12.6.2 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.

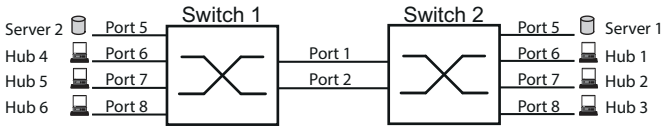


Figure 45: Link Aggregation Switch to Switch Network

Set up 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 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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	To add port `1/1` to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	To add port `1/2` to the Link Aggregation Group.

12.7 Link Backup

Link Backup provides a redundant link for the data packets on Layer 2 devices. When the device detects an error on the primary link, the device transfers the data packets 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 (STP) is disabled on the Link Backup ports.

12.7.1 Fail Back Description

Link Backup also lets you set up a Fail Back option. When you activate the *Fail back* function and the *Primary port* returns to normal operation, the device first blocks the data packets on the *Backup port* and then forwards the data packets to 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 the data packets, first sends a *Topology Change* packet to the remote device. The *Topology Change* packet helps the remote device quickly relearn the MAC addresses.

12.7.2 Application example for the Link Backup function

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 the data packets and the other port is in the *blocking* state.

The *Primary port* `2/3` on Switch A, is the active port and is forwarding the data packets to port 1 on Switch B. Port `2/4` on Switch A is the *Backup port* and blocks the data packets.

When Switch A disables port 2/3 because of a detected error, port 2/4 on Switch A starts forwarding data packets 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 data packets and then port 2/3 starts forwarding data packets.

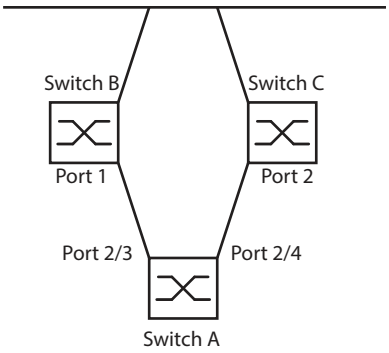


Figure 46: Link Backup example network

The following tables contain examples of parameters to set up Switch A.

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > Link Backup* dialog.
- ☐ 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.
- ☐ In the *Description* textbox, enter Link_Backup_1 as the name for the backup pair.
- ☐ To activate the *Fail back* function for the link backup pair, mark the *Fail back* checkbox.
- ☐ Set the fail back timer for the link backup pair, enter 30 s in *Fail back delay [s]*.
- ☐ To activate the link backup pair, mark the *Active* checkbox.
- ☐ Enable the *Link Backup* function.
  Select the *On* radio button in the *Operation* frame.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/3`	To change to the Interface Configuration mode of interface 2/3.
`link-backup add 2/4`	To add a Link Backup instance where port 2/3 is the *Primary port* and port 2/4 is the *Backup port*.
`link-backup modify 2/4 description Link_Backup_1`	To specify the string Link_Backup_1 as the name of the backup pair.
`link-backup modify 2/4 failback-status enable`	To enable the fail back timer.
`link-backup modify 2/4 failback-time 30`	To specify the fail back delay time as 30 s.

`link-backup modify 2/4 status enable`	To enable the Link Backup instance.
`exit`	To change to the Configuration mode.
`link-backup operation`	To enable the *Link Backup* function globally in the device.

12.8 FuseNet function

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- HIPER Ring
- RSTP

Note:
The prerequisite for coupling a network to the main ring using the *Ring/Network Coupling* function is that the connected network contains only network devices that support the *Ring/Network Coupling* function.

Use the following table to select the *FuseNet* coupling protocol to be used in the network:

Main Ring	Connected Network		
	MRP	**HIPER Ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *RCP* – *Ring/Network Coupling*	– *RCP* – *Ring/Network Coupling*
HIPER Ring	*Sub Ring*	*Ring/Network Coupling*	– *RCP* – *Ring/Network Coupling*
RSTP	*RCP*	*RCP*	–

– no suitable coupling protocol

1) with the *MRP* function set-up on different VLANs

12.9 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
- HIPER Ring

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.

12.9.1 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).

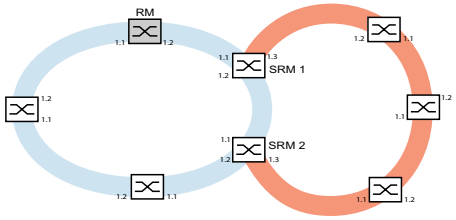


Figure 47: Example of a Sub Ring structure
blue ring = Main ring
orange ring = Sub Ring
SRM = Sub Ring Manager
RM = Ring Manager

The *Sub Ring Manager* capable devices support up to 20 instances and thus manage up to 20 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, in addition to the *Sub Ring Manager* devices themselves and the devices between the *Sub Ring Manager* devices in the main ring.

The following figures display examples of possible Sub Ring topologies:

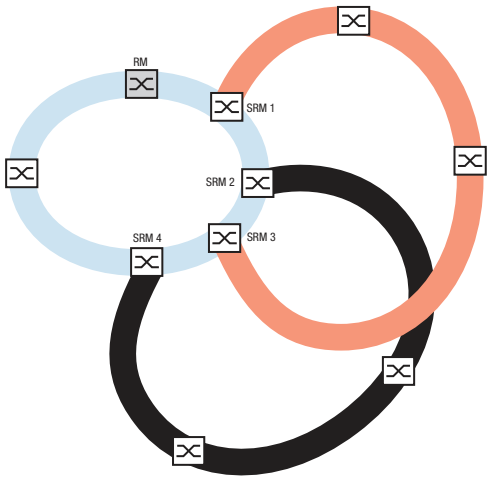


Figure 48: Example of an overlapping Sub Ring structure

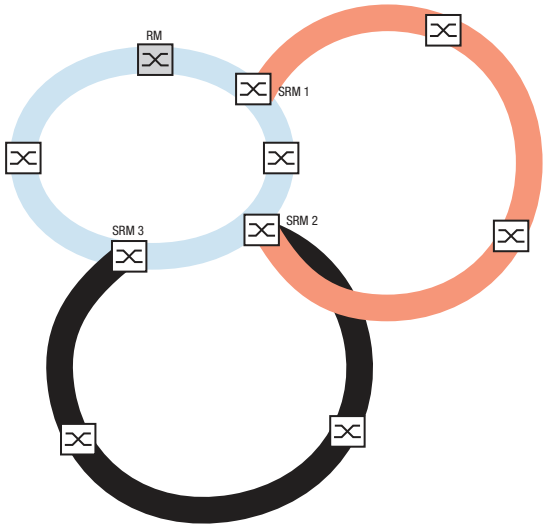


Figure 49: Special case: A Sub Ring Manager device manages 2 Sub Rings (2 instances). The Sub Ring Manager device is capable of managing up to 20 instances.

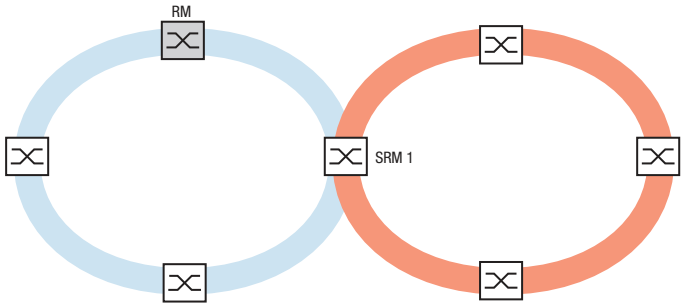


Figure 50: Special case: A Sub Ring Manager device manages both ends of a Sub Ring on different ports (Single Sub Ring Manger).

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* device
- VLAN `Y` for the Sub Ring (another VLAN ID than VLAN `X`)
  - on the ring ports of the devices participating in the Sub Ring
  - on the Sub Ring ports of the *Sub Ring Manager* device

  You can use the same VLAN for multiple Sub Rings.

12.9.2 Advanced Information

Sub Ring Packets

The Sub Ring protocol uses *Test*, *Link Change*, and *Topology Change* (*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 MAC address table (forwarding database) and sends *Topology Change* packets to the Sub Ring participants. The *Topology Change* packets prompt the devices participating in the Sub Ring to flush their MAC address table (forwarding database), too. This procedure helps forward the payload packets over the new path more quickly. This procedure applies regardless of whether the Sub Ring reconfiguration was caused by a *Link Down* or a *Link Up* notification.

Table 34: Sub Ring Packets

Packet Type	Send Mode	Time Parameter	Value
Test packet	Periodically	Send interval	40 ms[1]
		Reception timeout	280 ms[2]
Link Down packet[3]	Event-driven	On link-down of a Sub Ring port	-
Topology Change packet[4]	Event-driven	On Sub Ring reconfiguration	-

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 devices participating in the Sub Ring to flush their MAC address table (forwarding database).

Sub Ring Packet Prioritization

The devices participating in the Sub Ring 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 forward and send 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 ≥1.
- ☐ Specify the Sub Ring ports as T (tagged) members of this VLAN.

Note:
When you set the VLAN ID for the Sub Ring packets to a value ≥1 in the *Switching > L2-Redundancy > FuseNet > Sub Ring* dialog, the device adds its Sub Ring ports as T (tagged) members of this VLAN. If the VLAN does not yet exist, the device automatically sets up 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.

12.9.3 Sub Ring example

In the following example, you couple a new network segment with 3 devices to an existing main ring which uses the Media Redundancy Protocol (MRP). 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.

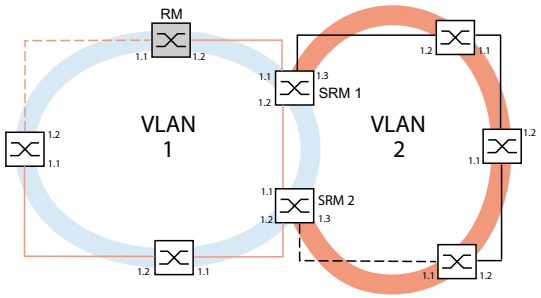


Figure 51: Example of a Sub Ring structure with VLANs
orange line= Main ring members in VLAN 1
black line= Sub Ring members in VLAN 2
orange dashed line= Main ring loop open
black dashed line= Sub Ring loop open
SRM = Sub Ring Manager
RM = Ring Manager

To set up the Sub Ring, perform the following steps:

- ☐ Set up 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, set up the speed and duplex mode of the ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up *100M 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* function on the devices participating in the main ring and Sub Ring. After you completely set up every device participating in the main ring and Sub Rings, activate the global *Sub Ring* function in the *Sub Ring Manager* devices.
- ☐ 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, set up the speed and duplex mode of the Sub Ring ports as follows:
  - For 100 Mbit/s TX ports, disable Automatic Negotiation and manually set up *100M 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 Media Redundancy Protocol (MRP). 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. Add 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 devices participating in the main ring and Sub Ring.
  - In the *Switching > L2-Redundancy > MRP* dialog, select the 2 ports participating in the main ring on the devices participating in the main ring.
  - For the devices participating in the Sub Ring use the steps above and set up the 2 ports participating in the Sub Ring.
  - Assign the same MRP domain ID to the devices participating in the main ring and Sub Ring. 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. As an alternative, you can use the Command Line Interface. To do this, perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain delete`	To delete the current MRP domain.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	To add an MRP domain with the specified MRP domain ID. Any subsequent MRP domain changes apply to this domain ID.

12.9.4 Application example for the Sub Ring function

Note:
Help avoid loops during configuration. Set up every device of the Sub Ring individually. Before you activate the redundant link, completely set up every device participating in the Sub Ring.

Set up the 2 *Sub Ring Manager* devices 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 *Administrative mode* column, select the *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* device.
  The options for the coupling are:
  - `manager`
    When you specify both *Sub Ring Manager* devices 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 the other *Sub Ring Manager* device operates in the *`manager`* mode. Otherwise the device with the higher MAC address manages the redundant link.

  Specify for *Sub Ring Manager* device 1 the value `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.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID `1`.
`sub-ring modify 1 port 1/3`	To specify port `1/3` as the Sub Ring port.
`sub-ring modify 1 name Test`	To assign the name `Test` to the Sub Ring `1`.
`sub-ring modify 1 mode manager`	To assign the `manager` mode to the Sub Ring `1`.
`show sub-ring ring`	To display the Sub Rings state on this device.
`show sub-ring global`	To display the Sub Ring global state on this device.

- ☐ Set up the second *Sub Ring Manager* device in the same way.
  Specify for *Sub Ring Manager* device 2 the value `redundant manager`, in accordance with the figure depicting this example.

- ☐ To activate the *Sub Ring Manager* mode, mark the *Active* checkbox in the corresponding table row.
- ☐ After you have set up both *Sub Ring Manager* devices and the devices participating in the Sub Ring, enable the function and close the redundant link.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring enable 1`	To activate Sub Ring `1`.
`sub-ring enable 2`	To activate Sub Ring `2`.
`exit`	To change to the Privileged EXEC mode.
`show sub-ring ring <Domain ID>`	To display the settings of the selected Sub Rings.
`show sub-ring global`	To display global Sub Ring settings.
`copy config running-config nvm profile Test`	To save the current settings in the configuration profile named `Test` in the non-volatile memory (`nvm`).

12.9.5 Cascaded Sub Rings example

The following example displays a cascaded Sub Ring network topology which uses the MRP and the SRM protocol. You couple the new network segments as Sub Rings to the existing devices of the main ring.

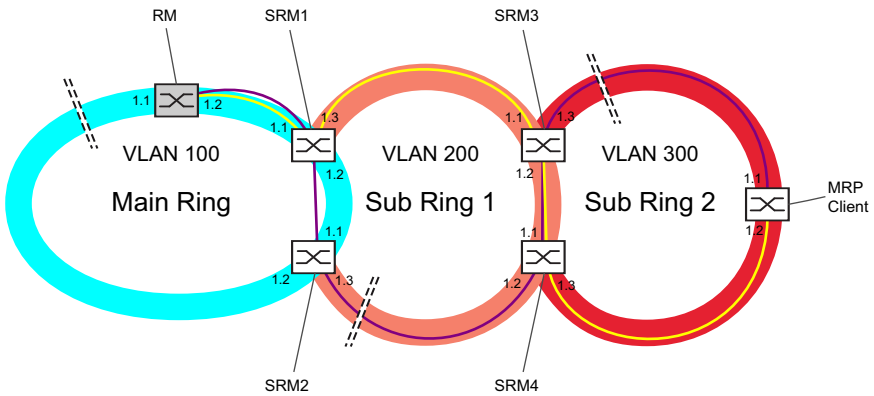


Figure 52: Example of a cascaded Sub Ring structure
Blue circle = Main ring members in VLAN 100
Orange circle = Sub Ring members in VLAN 200
Red circle = Sub Ring members in VLAN 300
Yellow line = Main network link
Purple line = Redundant network link
Dashed black lines = Blocked network link
SRM1 = Sub Ring Manager for Sub Ring 1 and MRP client for the Main Ring
SRM2 = Redundant Sub Ring Manager for Sub Ring 1 and MRP client for the Main Ring
SRM3 = Redundant Sub Ring Manager for Sub Ring 2 and MRP client for Sub Ring 1
SRM4 = Sub Ring Manager for Sub Ring 2 and MRP client for Sub Ring 1
MRP Client = MRP Client participating in Sub Ring 2
RM = Ring Manager

The configuration for this example is split into the following parts:
- Setting up the Ring Manager mode
- Setting up the devices participating in the Sub Ring

Setting up the Ring Manager mode

This example guides you through the configuration of the *Ring Manager* mode as shown above. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ Select port `1/1` in the *Ring port 1* frame and port `1/2` in the *Ring port 2* frame.
- ☐ Enable the *Ring manager* function.
  Select the *On* radio button in the *Configuration* frame.
- ☐ Assign the value `100` in the *VLAN ID* field.
- ☐ Enable the *MRP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab.
- ☐ To disable the *Spanning Tree* function on the ring ports, in the *STP active* column, unmark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain delete`	To delete the current MRP domain.
`mrp domain add default-domain`	To add a default MRP domain. Any subsequent MRP domain changes apply to this domain ID.
`mrp domain modify port primary 1/1`	To set up the primary ring port.
`mrp domain modify port secondary 1/2`	To set up the secondary ring port.
`mrp domain modify mode manager`	To enable the *Ring manager* function.
`mrp domain modify operation enable`	To enable the *MRP* function.
`mrp domain modify vlan 100`	To assign the VLAN ID to the ring ports.
`interface 1/1 spanning-tree mode disable`	To disable Spanning Tree on interface `1/1`.
`interface 1/2 spanning-tree mode disable`	To disable Spanning Tree on interface `1/2`.

Specify a different VLAN membership for the main ring and the Sub Rings. For example, use VLAN ID `100` for the main ring, VLAN ID `200` for the first Sub Ring and VLAN ID `300` for the second Sub Ring.

Setting up the devices participating in the Sub Ring

Set up each device participating in the Sub Ring in the same way. To do this, perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *MRP* dialog.
- ☐ From the *Port* drop-down list, select port `1/1` in the *Ring port 1* frame and port `1/2` in the *Ring port 2* frame.
- ☐ Disable the *Ring manager* function.
  Select the *Off* radio button in the *Operation* frame (if this has not already been done).
- ☐ Assign the value `100` in the *VLAN ID* field.
- ☐ Enable the *MRP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Switching* > *L2-Redundancy* > *FuseNet* > *Sub Ring* dialog.
- ☐ To add a table row, click the button.
- ☐ In the *Name* column, assign a name to the Sub Ring.
- ☐ In the *Port* column, select the appropriate port for which the device operates in the *Sub Ring Manager* mode.
  In the given example you use port `1/3`.
- ☐ Assign the value `200` in the *VLAN* column.
- ☐ In the *Administrative mode* column, select the value *manager*.
  You thus specify which port for coupling the Sub Ring to the main ring becomes the redundant manager.
  The options for the coupling are:
  - `manager`
    When you specify both *Sub Ring Manager* devices 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 the other *Sub Ring Manager* device operates in the *manager* mode. Otherwise the device with the higher MAC address manages the redundant link.
- ☐ To activate the Sub Ring, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *CIST* tab.
- ☐ To disable the *Spanning Tree* function on the Sub Ring ports, in the *STP active* column, unmark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring modify 1 port 1/3`	To specify port `1/3` as the Sub Ring port.
`sub-ring modify 1 name Test`	To assign the name `Test` to the Sub Ring.
`sub-ring add 1 mode manager vlan 200 port 1/3 name SRM1`	To assign the `manager` mode to the Sub Ring `1`.
`sub-ring enable 1`	To activate the Sub Ring.
`sub-ring operation enable`	To enable the *Sub Ring* function.

`interface 1/3 spanning-tree mode disable`	To disable Spanning Tree on interface `1/3`.
`show sub-ring ring`	To display the Sub Ring state on this device.
`show sub-ring global`	To display the Sub Ring global state on this device.

12.9.6 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* function.

Application example for Sub Ring with LAG

The following example is a simple setup between an MRP Ring and a Sub Ring.

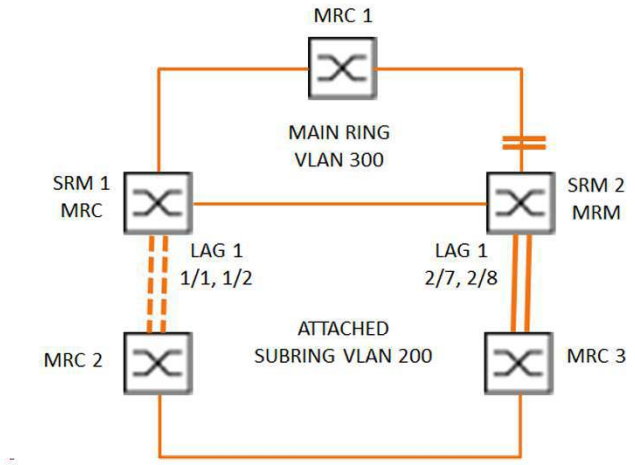


Figure 53: Sub Ring with Link Aggregation

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 35: Devices, Ports and Roles

Device Name	Ring Port	Main Ring Role	Sub Ring Role	Sub Ring Port
MRC1	1/3, 1/4	MRP client	-	-
SRM1	1/3, 1/4	MRP client	Redundant Manager	lag/1
SRM2	2/4, 2/5	MRP manager	Manager	lag/1
MRC2	lag/1, 1/3	-	MRP client	-
MRC3	lag/1, 1/3	-	MRP client	-

MRP Ring configuration

The devices participating in the Main ring are members of VLAN 300.

Perform the following steps:

SRM2

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID `default-domain`.
`mrp domain modify port primary 2/4`	To specify port `2/4` as *primary* ring port.
`mrp domain modify port secondary 2/5`	To specify port `2/5` as *secondary* ring port.
`mrp domain modify mode manager`	To designate the device as the *Ring Manager* device. Do not activate the *Ring manager* function on any other device.
`mrp domain modify operation enable`	To activate the MRP Ring.
`mrp domain modify vlan 300`	To specify the VLAN ID as `300`.
`mrp operation`	To enable the *MRP* function in the device.

MRC1, SRM1

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID `default-domain`.
`mrp domain modify port primary 1/3`	To specify port `1/3` as *primary* ring port.
`mrp domain modify port secondary 1/4`	To specify port `1/4` as *secondary* ring port.
`mrp domain modify mode client`	To set up the device as a *Ring Client* device.
`mrp domain modify operation enable`	To activate the MRP Ring.
`mrp domain modify vlan 300`	To specify the VLAN ID as `300`.
`mrp operation`	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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	To add port `1/1` to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 1/2`	To add port `1/2` to the Link Aggregation Group.
`link-aggregation modify lag/1 adminmode`	To activate the Link Aggregation Group.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID `1`.
`sub-ring modify 1 name SRM1`	To assign the name `SRM1` to the Sub Ring `1`.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/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`.
`sub-ring enable 1`	To activate Sub Ring `1`.
`sub-ring operation`	To enable the global *Sub Ring Manager* function on this device.

SRM2

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`link-aggregation add lag/1`	To add a Link Aggregation Group `lag/1`.
`link-aggregation modify lag/1 addport 2/7`	To add port `2/7` to the Link Aggregation Group.
`link-aggregation modify lag/1 addport 2/8`	To add port `2/8` to the Link Aggregation Group.
`link-aggregation modify lag/1 adminmode`	To activate the Link Aggregation Group.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sub-ring add 1`	To add a Sub Ring with the Sub Ring ID `1`.
`sub-ring modify 1 mode manager vlan 200 port lag/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`.
`sub-ring modify 1 name SRM2`	To assign the name `SRM2` to the Sub Ring `1`.
`sub-ring enable 1`	To activate Sub Ring `1`.
`sub-ring operation`	To enable the global *Sub Ring Manager* function on this device.

MRC 2, 3

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add an MRP domain with the ID `default-domain`.
`mrp domain modify port primary lag/1`	To specify port `lag/1` as *primary* ring port.
`mrp domain modify port secondary 1/3`	To specify port `1/3` as *secondary* ring port.
`mrp domain modify mode client`	To set up the device as a *Ring Client* device.
`mrp domain modify operation  enable`	To activate the MRP Ring.
`mrp domain modify vlan 200`	To specify the VLAN ID as `200`.
`mrp operation`	To enable the *MRP* function in the device.

Disabling 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/3`	To change to the Interface Configuration mode of interface `1/3`.
`no spanning-tree operation`	To disable the *Spanning Tree* function on the port.

12.10 Ring/Network Coupling function

Based on a ring, the *Ring/Network Coupling* function couples rings or network segments redundantly. *Ring/Network Coupling* connects 2 rings/network segments through 2 separate paths.

When the devices in the coupled network are Hirschmann devices, the *Ring/Network Coupling* function supports the coupling following ring protocols in the primary and secondary rings:
- HIPER Ring
- Fast HIPER Ring
- MRP

The *Ring/Network Coupling* function can also couple network segments of a bus and mesh structures.

12.10.1 Methods of Ring/Network Coupling

1-Switch coupling

Two ports of **one** device in the first ring/network connect to one port each of two devices in the second ring/network. See figure 61 on page 275.

In the 1-Switch coupling method, the main line forwards data and the device blocks the redundant line.

When the main line no longer functions, the device immediately unblocks the redundant line. When the main line is restored, the device blocks data on the redundant line. The main line forwards data again.

The ring coupling detects and handles an error within 500 ms (typically 150 ms).

2-Switch coupling

One port each from **two** devices in the first ring/network connects to one port each of two devices in the second ring/network segment. See figure 63 on page 278.

The device with the redundant line connected and the device with the main line connected use control packets to inform each other about their operating states, using the existing network or a dedicated control line.

When the main line goes down, the redundant device (Stand-by) unblocks the redundant line. When the main line comes up again, the device connected to the main line informs the redundant device of this. The Stand-by device then again blocks data on the redundant line. The device connected to the main line then again forwards data on the main line.

The ring coupling detects and handles a fault within 500 ms (typically 150 ms).

Selection of a coupling method

The type of coupling configuration is primarily determined by the network topological and the desired level of availability.

Table 36: Selection criteria for the configuration types for redundant coupling

	1-Switch coupling	2-Switch coupling	2-Switch coupling with Control line
Application	The 2 devices are in impractical topological positions. Therefore, putting a link between the devices would involve a lot of effort for 2-Switch coupling.	The 2 devices are in practical topological positions. Installing a control line would involve a lot of effort.	The 2 devices are in practical topological positions. Installing a control line would not involve much effort.
Disadvantage	If the Switch set up for the redundant coupling becomes inoperable, then no connection remains between the networks.	More effort is needed to connect both devices to the network (compared with 1-Switch coupling).	More effort is needed to connect both devices to the network (compared with 1-Switch and 2-Switch coupling).
Advantage	Less effort involved in connecting the 2 devices to the network (compared with 2-Switch coupling).	When one of the devices set up for the redundant coupling becomes inoperable, the coupled networks are still connected.	When one of the devices set up for the redundant coupling becomes inoperable, the coupled networks are still connected. The partner determination between the coupling devices occurs more reliable and faster than without the control line.

12.10.2 Advanced Information

Link Topology of 1-Switch coupling

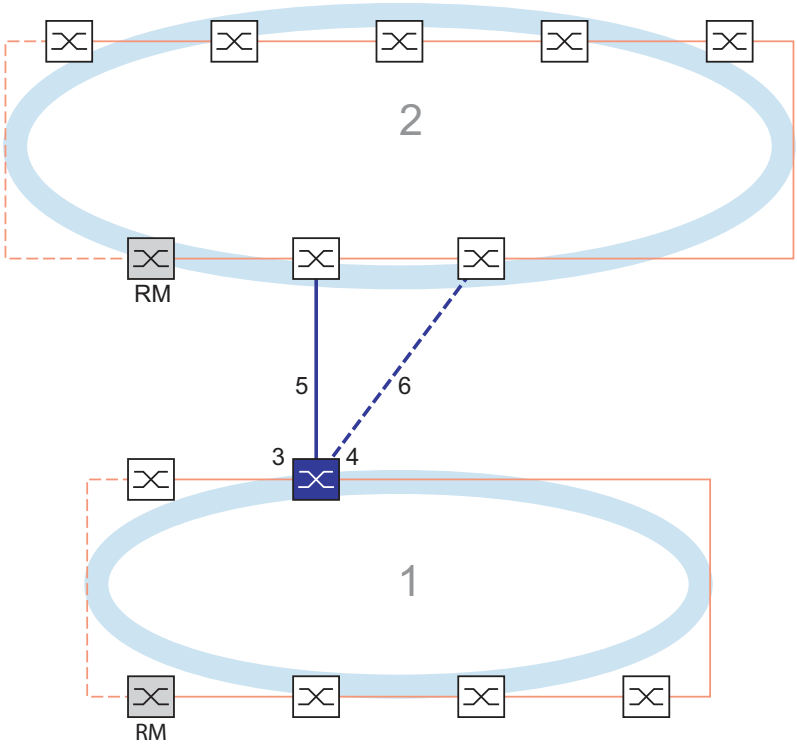


Figure 54: Example of 1-Switch coupling
1: Ring
2: Backbone
3: Partner coupling port
4: Coupling port
5: Main line
6: Redundant line

In a 1-Switch coupling (see figure 54), one device manages both coupling lines:
- The partner coupling port (3) connects the main line (5).
- The coupling port (4) connects the redundant line (6).

The single coupling device sends the following test packets:
- The partner coupling port (3) sends *Ring/Network Coupling* unicast test packets A.
- The coupling port (4) sends *Ring/Network Coupling* unicast test packets B.

Note:
The 2 ring ports (unnumbered) connect the local redundant ring (red lines in graphic) and do not send any *Ring/Network Coupling* test packets.

Link Topology of 2-Switch coupling

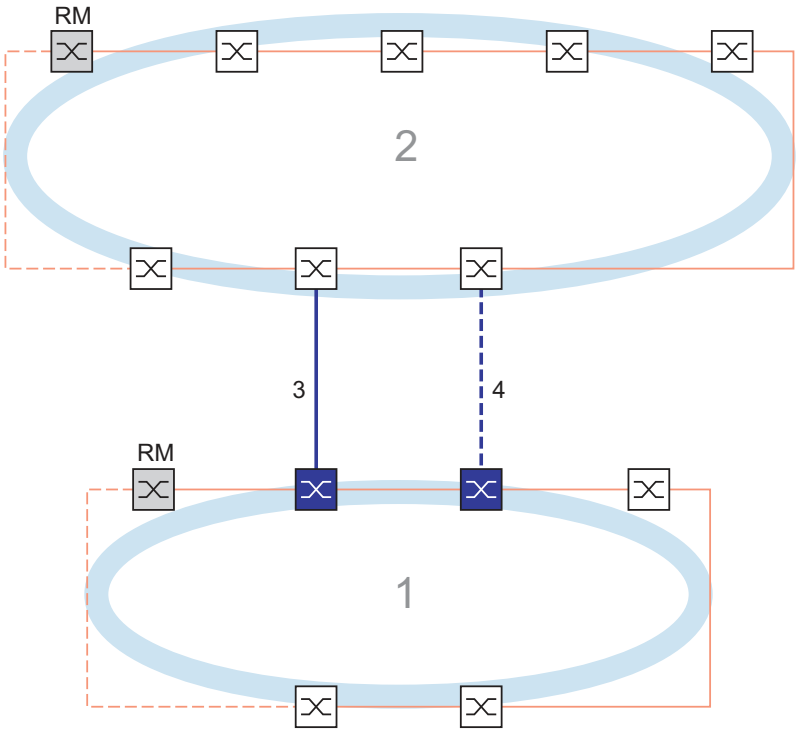


Figure 55: Example of 2-Switch coupling
1: Ring
2: Backbone
3: Main line
4: Redundant line

In a 2-Switch coupling (see figure 55), the 2 devices have specific roles:
- The coupling port (1) of the primary device connects the main line (see figure 56).
- The partner coupling port (1) of the secondary device connects the stand-by line (4) (see figure 57).

The primary device (see figure 56) sends no test packets.

The secondary device (see figure 57) sends the following test packets:
- The 2 ring ports (unnumbered) send *Ring/Network Coupling* unicast test packets A.
- The coupling port (4) sends *Ring/Network Coupling* unicast test packets B.

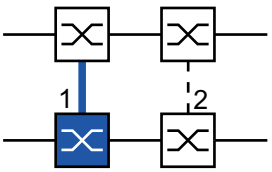


Figure 56: 2-Switch coupling, Primary device
1: Coupling port
2: Partner coupling port

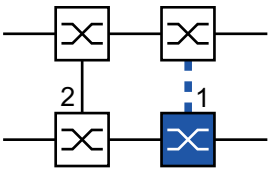


Figure 57: 2-Switch coupling, Stand-by device
1: Coupling port
2: Partner coupling port

Link Topology of 2-Switch coupling with Control Line

This topology differs from the previous one by the additional control line. The control line helps speed up reconfiguration.

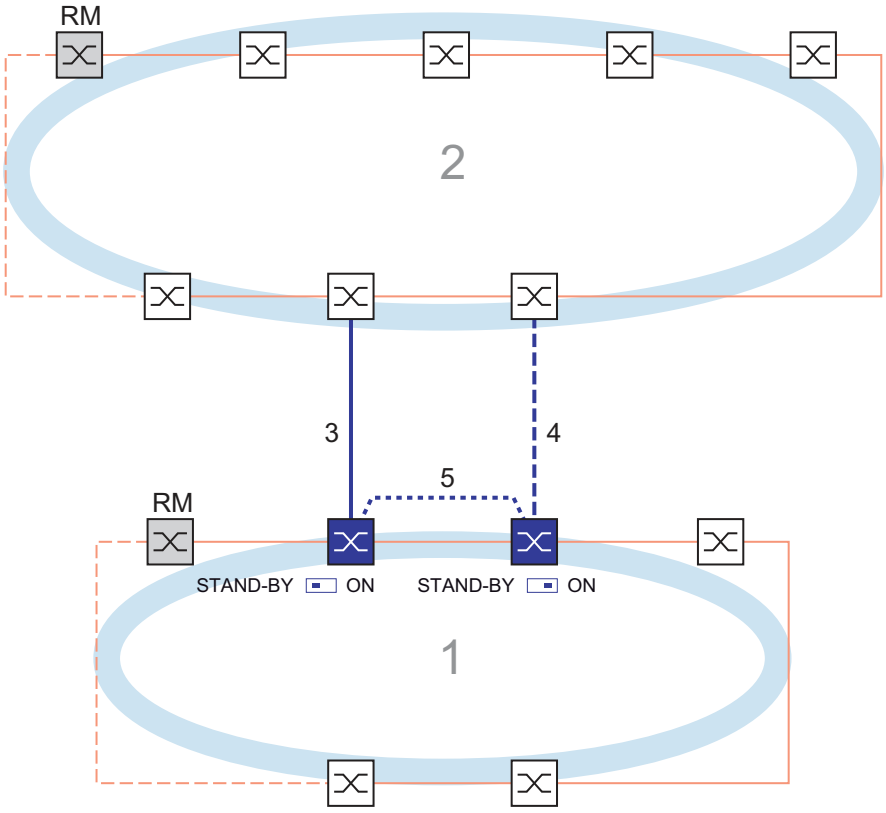


Figure 58: Example of 2-Switch coupling with control line
1: Ring
2: Backbone
3: Main line
4: Redundant line
5: Control line

In a 2-Switch coupling with Control Line (see figure 58), both devices are connected as follows:

- The primary device and the secondary device connect the control line (5) through their control ports (unnumbered).
- The coupling port (1) of the primary device connects the main line (see figure 59).
- The partner coupling port (1) of the secondary device connects the stand-by line (4) (see figure 60).

The primary device (see figure 59) sends control packets on its control port.

The secondary device (see figure 60) sends the following packets:
- The control port (unnumbered) sends control packets.
- The 2 ring ports (unnumbered) send *Ring/Network Coupling* unicast test packets A.
- The coupling port (4) sends *Ring/Network Coupling* unicast test packets B.

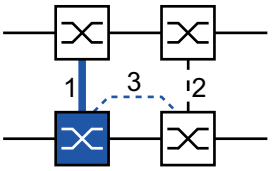


Figure 59: 2-Switch coupling with Control Line, Primary device
1: Coupling port
2: Partner coupling port
3: Control line

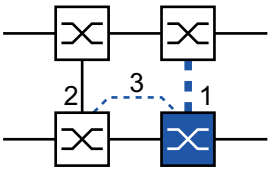


Figure 60: 2-Switch coupling with Control Line, Stand-by device
1: Coupling port
2: Partner coupling port
3: Control line

Packets

The *Ring/Network Coupling* function uses *Test*, *Control*, *Link Change*, and *Topology Change* packets.

Table 37: Ring/Network Coupling packets

Packet Type	Send Mode	Time Parameter	Value
Unicast test packet A[1]	Cyclical	Send interval	80 ms (50 ms during config. phase)
		Reception timeout	1500 ms
Unicast test packet B[2]	Cyclical	Send interval	80 ms (50 ms during config. phase)
		Reception timeout	1500 ms
Control packet[3]	Event-driven	On reconfiguration	-
Link Change packet[4]	Event-driven	On link-down or link-up of a ring port or coupling port	-
Topology Change packet	Event-driven	On reconfiguration	-

1. 2-Switch coupling: Sent by the secondary (stand-by) device only. Destination address: Device MAC address+1, source address: Device MAC address+2.
2. 2-Switch coupling: Sent by the secondary (stand-by) device only. Destination address: Device MAC address+2, source address: Device MAC address+1 (addresses swapped with respect to unicast test packet A).
3. Destination address (multicast): 01:80:63:07:00:02, source address: 00:80:63:07:10:01.
4. Sent by supporting ring participants.

1-Switch coupling: The local device periodically sends test packets A into the ring from both ring ports. The local device expects to receive the test packets A back on its respective other ring port. If the local device receives no test packets A for a specified amount of time, the local device detects a network failure.

The local device also sends test packets B from its partner coupling port. The test packets B are special packets that the local device receives at the coupling port although the coupling port blocks the reception of normal packets. The local device expects to receive the test packets B back on its coupling port. If the local device receives no test packets B for a specified amount of time, the local device detects a coupling network failure.

2-Switch coupling: The secondary (stand-by) device periodically sends test packets A into the ring from both ring ports. The secondary device expects to receive the test packets A back on its respective other ring port. If the secondary device receives no test packets A for a specified amount of time, the secondary device detects a network failure.

The secondary (stand-by) device also sends test packets B from its coupling port. The test packets B are special packets that the secondary device sends from its coupling port although the coupling port blocks the sending of normal packets. The primary device forwards received test packets B to the secondary device. The secondary device expects to receive the test packets B back on its ring port connected to the primary device. If the secondary device receives no test packets B for a specified amount of time, the secondary device detects a coupling network failure.

In extended redundancy mode, the same packets are used, only the reaction to a detected network failure differs.

On reconfiguration of the Ring/Network coupling, the secondary (stand-by) device flushes its MAC address table (forwarding database) and sends Ring/Network coupling *Topology Change* packets to its partner device. It also sends Ring/Network coupling *Topology Change* packets to the connected rings.

If a device participating in a connected ring receives a Ring/Network coupling *Topology Change* packet, it flushes its MAC address table (forwarding database). It also converts the Ring/Network coupling *Topology Change* packet to a ring *Topology Change* packet and sends the *Topology Change* packet on. The *Topology Change* packets prompt the other devices participating in the ring to flush their MAC address table (forwarding database), too. This applies to all rings that the Ring/Network coupling connects. This procedure helps forward the payload packets over the new path more quickly.

The Ring/Network coupling devices also act on ring *Topology Change* packets from a *Ring Manager* device because the Ring/Network coupling devices are members of that ring.

Packet Prioritization

The Ring/Network Coupling devices send their test packets, control packets, *Link Down* packets, and Ring/Network coupling *Topology Change* packets with the fixed VLAN ID 1. In the default setting, these packets are 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 the packets with the IEEE 802.1Q Class of Service priority 7 (Network control).

To prioritize these packets, set up each of the following ports as T (tagged) member of VLAN 1:
- In the local ring where the coupling device (or devices) are located:
  - The coupling port of the respective coupling device (local or secondary)
  - The partner coupling port of the respective coupling device (local or primary)
  - The ring ports of all devices in the local ring, including the *Ring Manager* device
- In the remote ring:
  - The port of the device in the remote ring connected to the coupling port
  - The port of the device in the remote ring connected to the partner coupling port
  - The 2 ring ports connecting the 2 devices just mentioned to each other

Note:
In a 2-Switch coupling with Control Line, the VLAN membership settings of both control ports must match. You can keep the default settings of the control ports (VLAN 1 membership untagged).

Link Topology Requirements

In the absence of packet prioritization, the following links must be direct, without any intervening devices:
- The 2 coupling links connecting the coupling device (or devices) in the local ring with the 2 coupled devices in the remote ring
- The link in the remote ring connecting the 2 coupled devices
- In a 2-Switch coupling: The link in the local ring connecting the 2 coupling devices
- In a 2-Switch coupling with Control Line, Hirschmann recommends to use a direct line but this is not strictly required.

This helps ensure that the packets are transmitted with minimal delay and high reliability. This again helps minimize the reconfiguration time under high network load.

Note:
Hirschmann recommends the above link topology even with packet prioritization.

12.10.3 Prepare the Ring/Network Coupling

Using the images in the dialog you define the role of the devices within the *Ring/Network Coupling*.

In the following screen shots and diagrams, the following conventions are used:
- Blue boxes and lines indicate devices or connections of the items currently being described.
- Solid lines indicate a main connection.
- Dash lines indicate a stand-by connection.
- Dotted lines indicate the control line.

Perform the following steps:

- Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- In the *Mode* frame, *Type* option list, select the required radio button.
  - *one-switch coupling*
  - *two-switch coupling, master*
  - *two-switch coupling, slave*
  - *two-switch coupling with control line, master*
  - *two-switch coupling with control line, slave*

Note:
Refrain from operating the *Spanning Tree* and the *Ring/Network Coupling* functions on the same ports.

1-Switch coupling

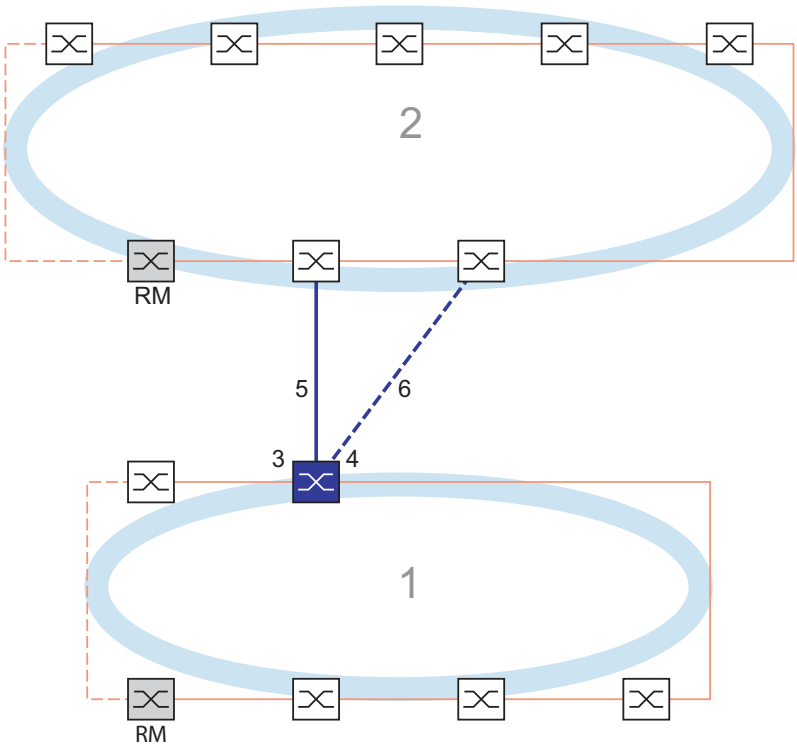


Figure 61: Example of 1-Switch coupling
1: Ring
2: Backbone
3: Partner coupling port
4: Coupling port
5: Main line
6: Redundant line

The main line, indicated by the solid blue line, which is connected to the partner coupling port provides coupling between the two networks in the normal mode of operation. If the main line is inoperable, then the redundant line, indicated by the dashed blue line, which is connected to the coupling port takes over the ring/network coupling. **One** switch performs the coupling switch-over.

The following settings apply to the device displayed in blue in the selected graphic.

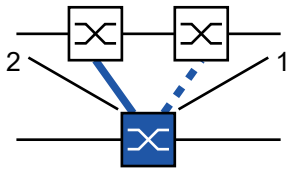


Figure 62: 1-switch coupling
1: Coupling port
2: Partner coupling port

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the *one-switch coupling* radio button.

Note:
Set up the *Partner coupling port* and the ring ports on different ports.

- ☐ In the *Coupling port* frame, select the port on which you want to connect the redundant line from the *Port* drop-down list.
- ☐ In the *Partner coupling port* frame, select the port on which you connect the main line from the *Port* drop-down list.
- ☐ Enable the *Ring/Network Coupling* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Connect the redundant line to the Partner coupling port.
  In the *Partner coupling port* frame, the *State* field displays the status of the Partner coupling port.
- ☐ Connect the main line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.

In the *Information* frame, the *Redundancy* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

For the coupling ports, perform the following steps:

Note:
The following settings are required for the coupling ports.

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Apply the settings temporarily. To do this, click the button.

To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:

- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify *100M FDX*.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, then specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID set up on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` table row.
- ☐ Apply the settings temporarily. To do this, click the button.

The coupling device now sends the redundancy packets with the highest priority on `VLAN 1`.

- ☐ In the *Configuration*frame, *Redundancy mode* option list, specify the type of redundancy:
  - With the *redundant ring/network coupling* setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - When you activate the *extended redundancy* setting, the main line and the redundant line can become active simultaneously if required. The setting lets you add redundancy to the remote (coupled) network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.

Note:
During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.

The *Coupling mode* describes the type of the backbone network to which you connect the ring network. See figure 61 on page 275.

- ☐ In the *Configuration* frame, *Coupling mode* option list, specify the type of the second network:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.
- ☐ Apply the settings temporarily. To do this, click the button.

You can reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the button.

2-Switch coupling

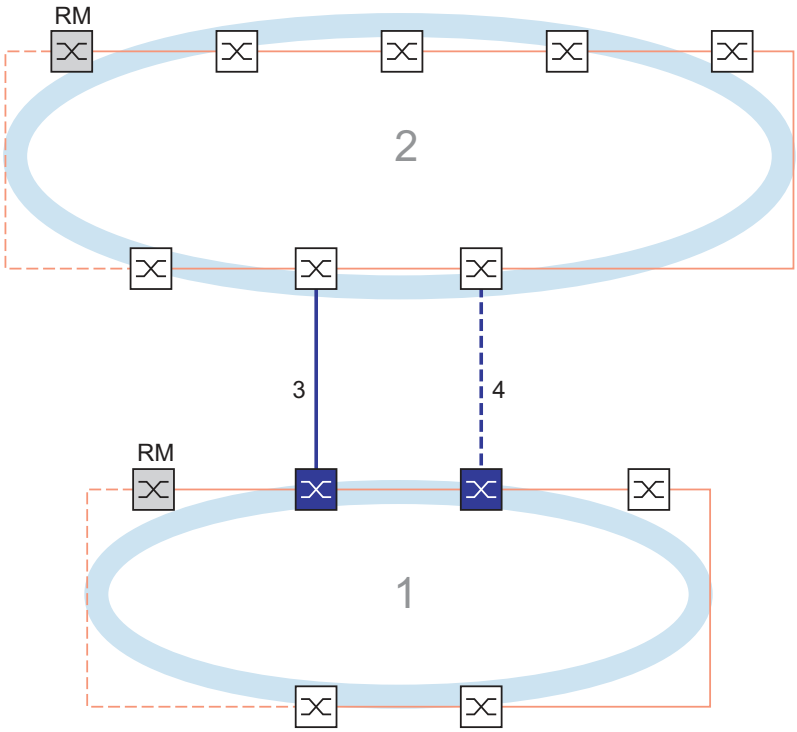


Figure 63: Example of 2-Switch coupling
1: Ring
2: Backbone
3: Main line
4: Redundant line

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the connected devices becomes inoperable, then the redundant line, indicated by the dashed black line, takes over the network coupling. The coupling is performed by 2 devices.

The devices send control packets to each other over the network.

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

☐ Connect the 2 partners using the ring ports.

2-Switch coupling, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

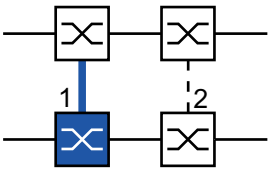


Figure 64: 2-Switch coupling, Primary device
1: Coupling port
2: Partner coupling port

Perform the following steps:

- ☐ Open the *Switching* > *L2-Redundancy* > *FuseNet* > *Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the `two-switch coupling, master` radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.
- ☐ Enable the *Ring/Network Coupling* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Connect the main line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings* > *Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:

- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify *100M FDX*.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, then specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID set up on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and to establish the VLAN membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` table row.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

The coupling device now sends the redundancy packets with the highest priority on `VLAN 1`.

2-Switch coupling, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

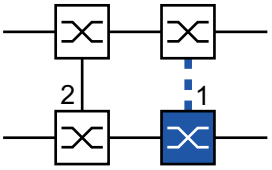


Figure 65: 2-Switch coupling, Stand-by device
1: Coupling port
2: Partner coupling port

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the *two-switch coupling, slave* radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.
- ☐ Enable the *Ring/Network Coupling* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Connect the redundant line to the *Coupling port*.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:
- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Apply the settings temporarily. To do this, click the button.

To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:
- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify *100M FDX*.
- For the other port types, keep the port-specific default settings.

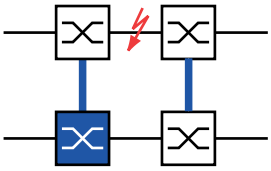
If you have set up VLANs on the coupling ports, then specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID set up on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` table row.
- ☐ Apply the settings temporarily. To do this, click the button.

The coupling devices now send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - *redundant ring/network coupling*
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - *extended redundancy*
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.

    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- ☐ In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network. See figure 63 on page 278.
- ☐ Apply the settings temporarily. To do this, click the button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the button.

2-Switch coupling with Control Line

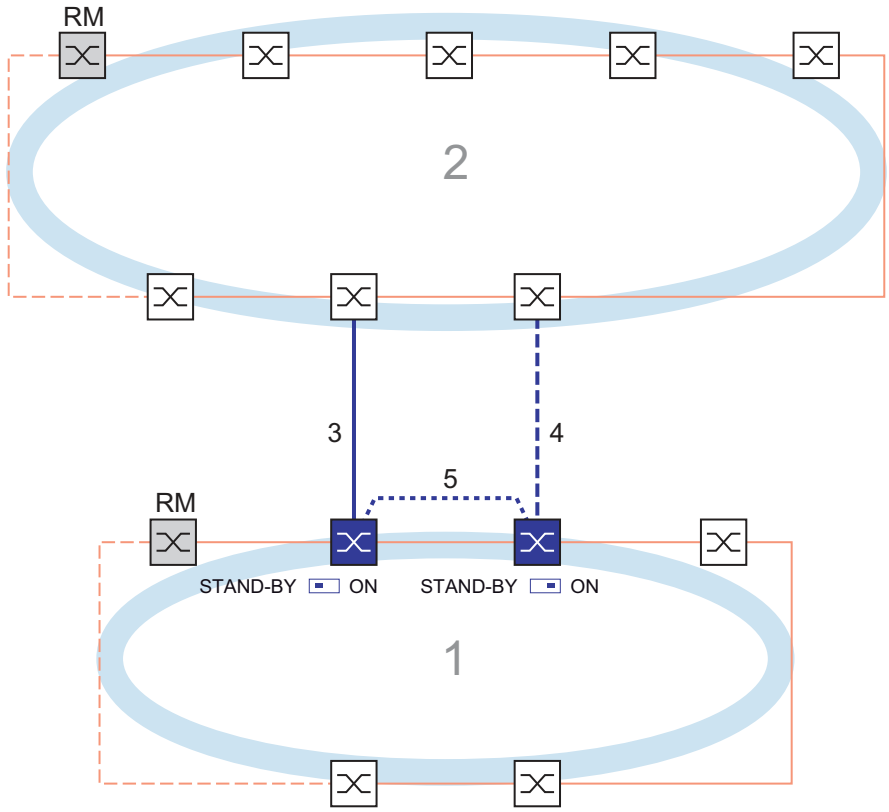


Figure 66: Example of 2-Switch coupling with control line
1: Ring
2: Backbone
3: Main line
4: Redundant line
5: Control line

The coupling between 2 networks is performed by the main line, indicated by the solid blue line. If the main line or one of the adjacent devices become inoperable, then the redundant line, indicated by the dashed blue line, takes over coupling the 2 networks. The ring coupling is performed by 2 devices.

The devices send control packets over a control line indicated by the dotted blue line. See figure 67 on page 283.

The primary device connected to the main line, and the stand-by device connected to the redundant line are partners with regard to the coupling.

☐ Connect the 2 partners using the ring ports.

2-Switch coupling with Control Line, Primary device

The following settings apply to the device displayed in blue in the selected graphic.

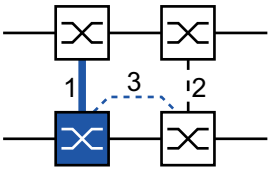


Figure 67: 2-Switch coupling with Control Line, Primary device
1: Coupling port
2: Partner coupling port
3: Control line

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the *two-switch coupling with control line, master* radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.
- ☐ In the *Control port* frame, select the port on which you connect the control line from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.
- ☐ Enable the *Ring/Network Coupling* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- ☐ Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

For the coupling ports, perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog, *Configuration* tab.
- ☐ For the ports selected as the coupling ports, specify the settings according to the parameters in the following table.
- ☐ Apply the settings temporarily. To do this, click the button.

To minimize the ring recovery time in case of a link-up after a failure, set up the speed and duplex mode of the ring ports as follows:
- For 100 Mbit/s TX ports, disable Automatic Negotiation and manually specify *100M FDX*.
- For the other port types, keep the port-specific default settings.

If you have set up VLANs on the coupling ports, then specify the VLAN settings on the coupling and partner coupling ports. To do this, perform the following steps:

- ☐ Open the *Switching > VLAN > Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID set up on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` table row.
- ☐ Apply the settings temporarily. To do this, click the button.

The coupling device now sends the redundancy packets with the highest priority on `VLAN 1`.

2-Switch coupling with Control Line, Stand-by device

The following settings apply to the device displayed in blue in the selected graphic.

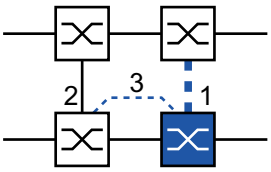


Figure 68: 2-Switch coupling with Control Line, Stand-by device
1: Coupling port
2: Partner coupling port
3: Control line

Perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Mode* frame, *Type* option list, select the *`two-switch coupling with control line, slave`* radio button.
- ☐ In the *Coupling port* frame, select the port on which you connect the network segments from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.

- ☐ In the *Control port* frame, select the port on which you connect the control line from the *Port* drop-down list.
  Set up the *Coupling port* and the ring ports on different ports.
- ☐ Enable the *Ring/Network Coupling* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Connect the redundant line to the Coupling port.
  In the *Coupling port* frame, the *State* field displays the status of the Coupling port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.
- ☐ Connect the control line to the Control port.
  In the *Control port* frame, the *State* field displays the status of the Control port.
  When the partner is already operating in the network, the *IP address* field in the *Partner coupling port* frame displays the IP address of the partner port.

In the *Information* frame, the *Redundancy* field displays if the redundancy is available. The *Configuration failure* field displays if the settings are complete and correct.

To help prevent continuous loops while the connections are in operation on the ring coupling ports, perform one of the following actions. The device sets the port state of the coupling port to “off”:

- disable the operation
- change the configuration

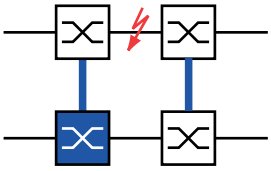
For the coupling ports, perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Port* dialog.
- ☐ Change the *Port-VLAN ID* setting to the value of the VLAN ID set up on the ports.
- ☐ Unmark the *Ingress filtering* checkbox for both coupling ports.
- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ To tag the redundant connections for `VLAN 1` and VLAN Membership, enter the value `T` in the cells corresponding to both coupling ports on the `VLAN 1` table row.
- ☐ Apply the settings temporarily. To do this, click the button.

The coupling devices now send the redundancy packets with the highest priority on `VLAN 1`.

Specify the *Redundancy mode* and *Coupling mode* settings. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > Ring/Network Coupling* dialog.
- ☐ In the *Configuration* frame, *Redundancy mode* option list, select one of the following radio buttons:
  - ▶ `redundant ring/network coupling`
    With this setting, either the main line or the redundant line is active. The setting lets the devices toggle between both lines.
  - ▶ `extended redundancy`
    With this setting, the main line and the redundant line are active simultaneously. The setting lets you add redundancy to the second network. When the connection between the coupling devices in the second network becomes inoperable, the coupling devices continue to transmit and receive data.

    During the reconfiguration period, packet duplications can occur. Therefore, select this setting only if your devices detect package duplications.
- ☐ In the *Configuration* frame, *Coupling mode* option list, select one of the following radio buttons:
  - ☐ If you connect to a ring network, then select the *ring coupling* radio button.
  - ☐ If you connect to a bus or mesh structure, then select the *network coupling* radio button.

  The *Coupling mode* describes the type of the backbone network to which you connect the ring network. See figure 66 on page 282.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Reset the coupling settings to the default state. To do this, perform the following steps:

- ☐ Click the 🗑 button.

12.11 RCP function

Industrial applications require the networks to have high availability. This includes deterministic, short interruption times in cases where a network device or link becomes inoperable.

A ring topology provides short transition times with a minimal use of resources. However, ring topologies bring the challenge of coupling these rings redundantly.

The Redundant Coupling Protocol (RCP) lets you couple rings that are operating with one of the following redundancy protocols:
- MRP
- HIPER Ring
- RSTP

The *RCP* function also lets you couple multiple secondary rings to a primary ring. See the following figure. Only the devices which couple the rings require the *RCP* function.

You can also use devices other than Hirschmann devices within the coupled networks.

The *RCP* function uses a master and a slave device to transport data packets between the networks. Only the master device forwards data packets between the rings.

Using Hirschmann proprietary multicast messages, the *RCP* master and slave devices inform each other about their operating state. Set up the devices in the secondary ring which are not coupling devices to forward the following multicast addresses:
- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Connect the master and slave devices as direct neighbors.

You use 4 ports per device to establish the redundant coupling. Set up the coupling devices with 2 inner and 2 outer ports in each network.

- The inner ports connect the master and slave devices.
- The outer ports connect the devices to the other, neighboring devices of the network.

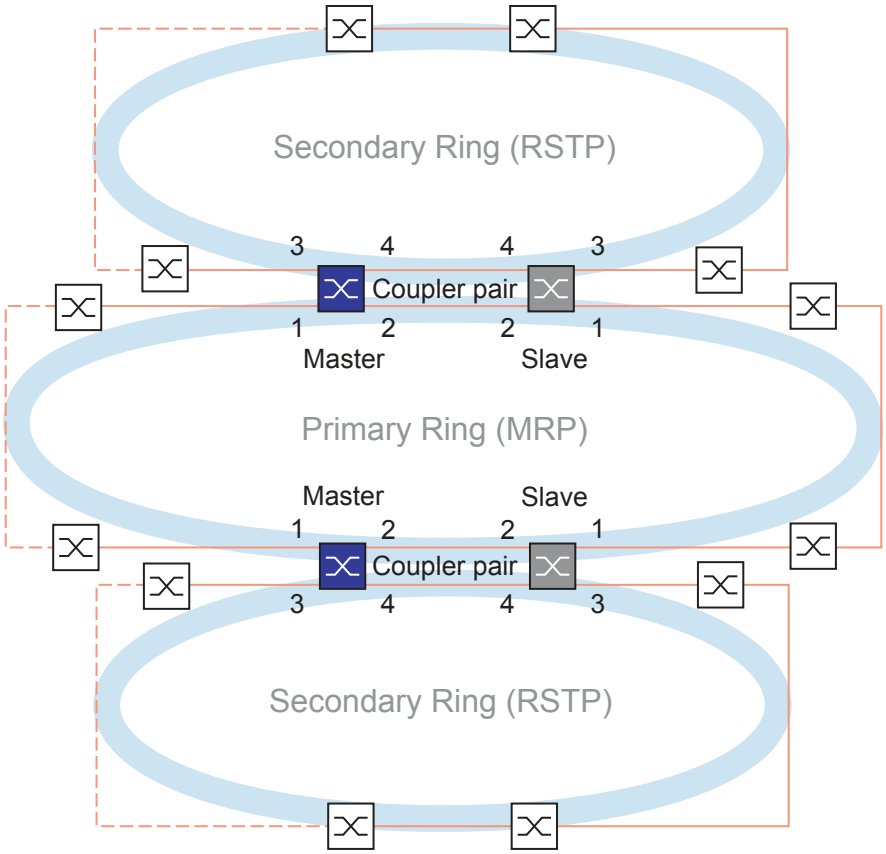


Figure 69: Example of a two-switch redundant coupling (2 coupler pairs)
1: Outer coupling port in the primary ring
2: Inner coupling port in the primary ring
3: Outer coupling port in the secondary ring
4: Inner coupling port in the secondary ring

When you specify the role of a coupler device as *auto*, the coupler device automatically selects its role as *master* or *slave*. When you want a predetermined master or slave device, specify the roles explicitly.

If the master device is no longer reachable through the inner coupling ports, the slave device waits for a specified timeout to expire before taking over the master role. During this period, the slave device continues attempting to reach the master device through the outer coupling ports. When the master device remains unreachable after the timeout period expires, the slave device takes over the master role. To maintain stability in the network connected to the outer coupling ports, specify the *RCP* timeout value longer than the recovery time of the coupled rings.

Note:
Disable RSTP on the *RCP* inner and outer ports that are not connected to the RSTP ring. In the example configuration, you disable RSTP on ports 1 and 2 of every device.

12.11.1 Prerequisites for RCP

Prerequisite for setting up an *RCP* coupler pair is that every device in the network (besides the coupler pair) supports the forwarding of untagged multicast packets.

12.11.2 Advanced Information

Topology Overview

RCP supports the following topology:
- Two-Switch Redundant Coupling

Note:
For a topology example with 2 instances of a Two-Switch Redundant Coupling (see figure 69).

This topology has the following characteristics:
- Each RCP device has 2 internal network segments:
  - A primary segment
  - A secondary segment
- In the normal state of operation, the RCP devices treat packets traveling between these 2 network segments as follows:
  - The RCP master device forwards packets between the 2 network segments.
  - The RCP slave device does **not** forward packets between the 2 network segments.
- Port associations:
  - Only the ports explicitly set up as inner or outer RCP ports for the secondary segment belong to the RCP secondary segment of the device.
  - The inner and outer RCP ports for the primary segment belong to the RCP primary segment.
  - All other ports implicitly belong to the RCP primary segment.
- The management of an RCP device is located in the primary segment.

Note:
If you want to access the management of an RCP slave device from the secondary segment, avoid the port-based routing function on the outer ports for the secondary segment. This helps you maintain the management access to the device from the secondary segment.

Topology of the Two-Switch Redundant Coupling

In a Two-Switch Redundant Coupling, one pair of devices couples the 2 rings. Each of the paired devices has a distinct coupling role master or slave, either automatically set up or explicitly specified.

The devices are connected as follows (see figure 69):
- The ring ports (1) of both devices connect to the primary ring/network. These ports are the outer ports for the primary network.
- The ring ports (2) of both devices connect to each other for the primary ring/network. These ports are the inner ports for the primary network.
- The ring ports (3) of both devices connect to the secondary ring/network. These ports are the outer ports for the secondary network.
- The ring ports (4) of both devices connect to each other for the secondary ring. These ports are the inner ports for the secondary network.

Packets

RCP uses multicast test packets, named after the RCP port role number (1..4) of the sending port.

Table 38: RCP Packets

Packet Type	Operating State	Time Parameter	Value
Test packets 2 and 4 (on the inner ports)	Normal operation of the inner ports	Send interval	45 ms
		Reception timeout[1]	180 ms (4 send intervals, fixed)
Test packets 1 and 3 (on the outer ports)	On link loss of the inner ports	Send interval	10 ms (during the first 90 ms of the reception timeout) 5 ms (after 90 ms of the reception timeout have elapsed)
		Topology Change timeout[2]	5 ms..60000 ms (customizable, default setting: 250 ms)

1. The slave treats the reception timeout as a link loss on the respective port even if the port still has a link.
2. After detecting a link loss, the slave device waits for the duration of the *Topology Change* timeout before forwarding packets between the 2 network segments.

Link Topology Requirements

The following links must be direct, without any other devices in between:

- The 2 links connecting the inner ports (2, 4) of each coupler pair in the respective primary and secondary rings.

This helps ensure that a link loss is quickly detected by the RCP devices.

12.11.3 Application example for RCP coupling

The Hirschmann devices support the two-switch redundant coupling. You can use the *RCP* function to provide a network installed in a train for example. The network provides information for the passengers about the train location or the different stops on the line. The network can also help provide passenger safety, for example using video surveillance.

The primary rings in the figure represent an *MRP* ring within each car. Each primary ring consists of 4 devices. See the following figure.

The secondary rings in the figure represent RSTP rings that automatically form when 2 cars are being coupled. Each secondary ring consists of 2 coupler pairs that are joined through their respective outer ports. In the figure, these device quadruples are called Coupler A and B.

To simplify the port configuration, the *MRP* ring ports and the *RCP* inner and outer ports are assigned the same port numbers on each switch. For example, on the switches 2A..2D, specify the ports `2/1` and `2/2` as MRP Ring ports, the ports `2/4` as *RCP* inner ports, and the ports `2/3` as *RCP* outer ports.

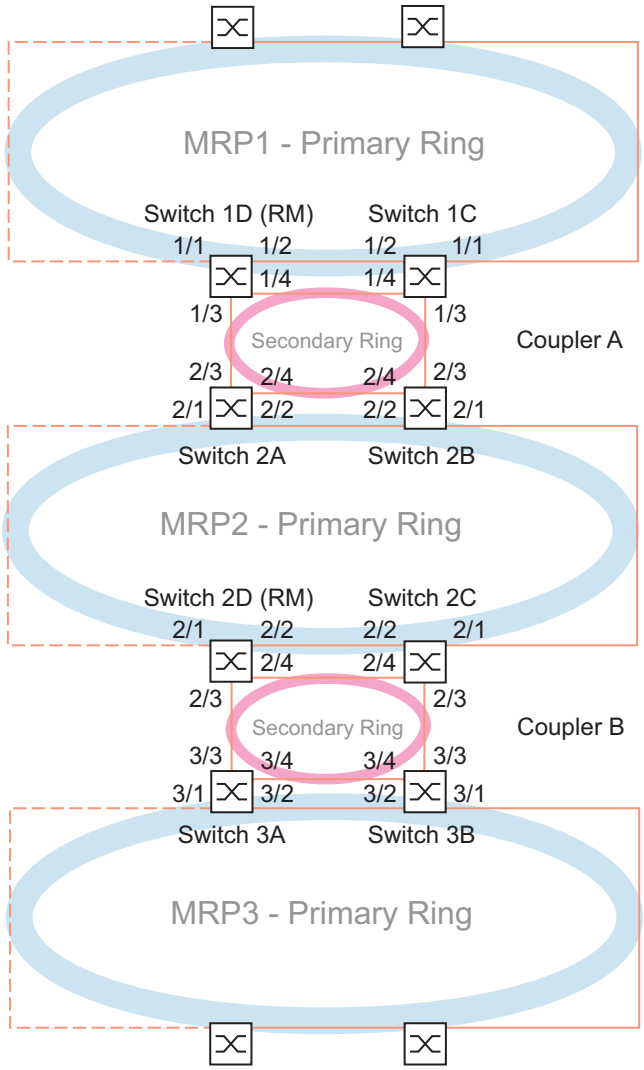


Figure 70: Redundant Coupling Protocol Train Topology:
- Ports x/1 and x/2 are MRP ring ports
- Ports x/3 are RCP outer ports
- Ports x/4 are RCP inner ports

The following steps describe how to specify the parameters for the railway car represented by the MRP2 ring.

Set up the switches 2A..2C as an MRP *Ring Client* device. Set up only switch 2D as the MRP *Ring Manager* device. Set up the switches 2A and 2B as one RCP coupler pair and the switches 2C and 2D as the second coupler pair.

Disabling the RSTP function on the MRP Ring ports

MRP and RSTP do not work together. Therefore, deactivate the RSTP function on the *RCP* ports used in the *MRP* ring. In the example configuration, ports `x/1` and `x/2` are used for the *MRP* ring. Activate the RSTP function only on the *RCP* inner and outer ports used in the secondary ring. For example, activate the RSTP function on the ports `x/3` and `x/4`.

If you disable the *MRP* function, then the device re-enables the RSTP function on the *RCP* ports used in the primary ring. In the example configuration, the device re-enables RSTP on ports `x/1` and `x/2`.

Note:
Substitute the port designation examples like `x/1` with the actual port numbers on your system. Depending on your device, the port designation may consist of only the port number.

Perform the following steps on the switches 2A..2D:

- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* dialog, *CIST* tab.
- ☐ In the default setting, the RSTP function is active on the ports. To deactivate the RSTP function on the *MRP* ring ports, unmark the *STP active* checkboxes for ports `x/1` and `x/2`.
- ☐ Open the *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* dialog.
- ☐ Enable the *Spanning Tree* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface x/1`	To change to the Interface Configuration mode of interface `x/1`.
`no spanning-tree mode`	To disable the *Spanning Tree* function on the port.
`exit`	To change to the Configuration mode.
`interface x/2`	To change to the Interface Configuration mode of interface `x/2`.
`no spanning-tree mode`	To disable the *Spanning Tree* function on the port.
`exit`	To change to the Configuration mode.
`spanning-tree operation`	To enable the *Spanning Tree* function.

Setting up the MRP Ring Manager and Ring Client devices

Set up the switches 2A..2C as an MRP *Ring Client* device. Set up only switch 2D as the MRP *Ring Manager* device. See figure 70 on page 291.

Set up the other switches in the rings as *Ring Client* devices. To do this, perform the following steps:

- ☐ Open the *Switching > L2-Redundancy > MRP* dialog.
- ☐ Specify the first ring port in the *Ring port 1* frame.
  From the *Port* drop-down list, select port `x/1`.
- ☐ Specify the second ring port in the *Ring port 2* frame.
  From the *Port* drop-down list, select port `x/2`.
- ☐ On switch 2D only: To designate the device as the MRP *Ring Manager* device, enable the *Ring manager* function. For switches 2A..2C, leave the default setting.
- ☐ Enable the *MRP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`mrp domain add default-domain`	To add a *MRP* domain with the ID `default-domain`.
`mrp domain modify port primary x/1`	To specify port `x/1` as *primary* ring port.
`mrp domain modify port secondary x/2`	To specify port `x/2` as *secondary* ring port.
`mrp domain modify mode manager`	On switch 2D only: To designate the device as the *Ring Manager* device. For switches 2A..2C, leave the default setting.
`mrp domain modify operation enable`	To enable the *MRP* function.

Specifying the ports for the RCP coupler pairs

Note:
The example leaves the roles of the coupler pair devices at the default value *auto*. The coupler pair devices then automatically select their roles as *master* or *slave*. When you want specific master or slave roles for a device pair, specify the roles explicitly.

Perform the following steps on the switches 2A..2D:

- ☐ Open the *Switching > L2-Redundancy > FuseNet > RCP* dialog.
- ☐ Specify the *Inner port* in the *Primary ring/network* frame.
  Select port `x/2`.
- ☐ Specify the *Outer port* in the *Primary ring/network* frame.
  Select port `x/1`.
- ☐ Specify the *Inner port* in the *Secondary ring/network* frame.
  Select port `x/4`.
- ☐ Specify the *Outer port* in the *Secondary ring/network* frame.
  Select port `x/3`.

- ☐ Enable the *RCP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`redundant-coupling port primary inner x/2`	To specify port `x/2` as the *primary inner* port.
`redundant-coupling port primary outer x/1`	To specify port `x/1` as the *primary outer* port.
`redundant-coupling port secondary inner x/4`	To specify port `x/4` as the *secondary inner* port.
`redundant-coupling port secondary outer x/3`	To specify port `x/3` as the *secondary outer* port.
`redundant-coupling operation`	To enable the *RCP* function in the device.

13 Tracking

The tracking function lets you monitor certain objects, such as the availability of an interface or reachability of a network.

Tracking can monitor the following objects:
- Link status of an interface (interface tracking)
- Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:
- up (OK)
- down (not OK)
- notReady (not enabled)

The definition of "up" and "down" depends on the type of the tracking object (for example interface tracking).

Tracking can forward the state changes of an object to the following applications:
- Static routing
- Interface status

13.1 Interface tracking

With interface tracking the device monitors the link status of:
- Physical ports
- Link Aggregation interfaces
- VLAN router interfaces

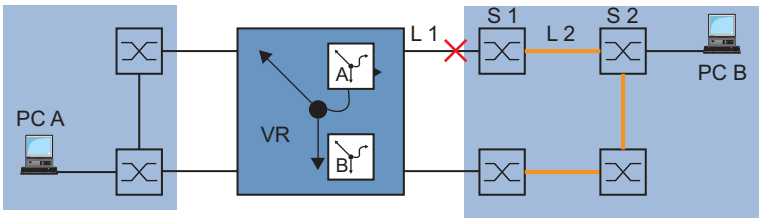


Figure 71: Monitoring a line with interface tracking

Ports/interfaces can have the following link statuses:
- interrupted physical link (link down)
- existing physical link (link up)

If the link to the participating ports is interrupted, then a Link Aggregation interface has link status “down”.

If the link is interrupted from the physical ports/Link Aggregation interfaces that are members of the corresponding VLAN, then the VLAN router interface has the link status “down”.

Setting a delay time lets you insert a delay before informing the application about an object status change.

If the physical link interruption remains for longer than the “link down delay” delay time, then the interface tracking object has the status “down”.

When the physical link holds for longer than the “link up delay” delay time, the interface tracking object has the status “up”.

State on delivery: delay times = 0 seconds.

This means that in case where a status changes, the registered application is informed immediately.

You can set the “link down delay” and “link up delay” delay times independently of each other in the range from 0 to 255 seconds.

You can define an interface tracking object for each interface.

13.2 Logical tracking

Logical tracking lets you logically link multiple tracking objects with each other and thus perform relatively complex monitoring tasks.

You can use logical tracking, for example, to monitor the link status for a network node to which redundant paths lead.

The device provides the following options for a logical link:
- *and*
- *or*

For a logical link, you can combine up to 2 operands with one operator.

Logical tracking objects can have the following statuses:
- The result of the logical link is incorrect (*down*).
- The result of the logical link is correct (*up*).
- The monitoring of the tracking object is inactive (*notReady*).

When a logical link delivers the result *down*, the device can choose to use an alternative path.

13.3 Configuring the tracking

You configure the tracking by setting up tracking objects. The following steps are required to set up a tracking object:

- Enter the tracking object ID number (track ID).
- Select a tracking type, for example interface.
- Depending on the track type, enter additional options such as “port” or “link up delay” in the interface tracking.

Note:
The registration of applications (for example VRRP) to which the tracking function reports status changes is performed in the application itself.

13.3.1 Configuring interface tracking

☐ Set up interface tracking on port `1/1` with a link down delay of `0` seconds and a link up delay of `3` seconds. To do this, perform the following steps:

☐ Open the *Advanced > Tracking > Configuration* dialog.

☐ Click the button.
The dialog displays the *Create* window.

Select type:

☐ Enter the values you desire, for example:
Type: `interface`
Track ID: `11`

☐ Click the *Ok* button.

Properties:

☐ Enter the values you desire, for example:
Port: `1/1`
Link up delay [s]: `3`
Link down delay [s]: `0`

☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`track add interface 11`	To add a tracking object to the table.
`track modify interface 11 ifnumber 1/1 link-up-delay 3 link-down-delay 0`	To specify the parameters for this tracking object.
`track enable interface 11`	To activate the tracking object.

```
Tracking ID interface-11 created  Target interface set to 1/1
  Link Up Delay for target interface set to 3 sec
  Link Down Delay for target interface set to 0 sec
Tracking ID 11 activated
```

```
exit                                          To change to the Privileged EXEC mode.
show track interface                          To display the set-up tracking objects.
Name     If-Number  Link-Up-Delay  Link-Down-Delay  State  Active
-------- ---------- -------------  ---------------  -----  ------
if-11     1/1                   0                3   up       [x]
```

13.4 Interface status application

The interface status application lets you control the status of one or more interfaces based on the status changes of a tracking object.

For example:
- When the status of the tracking object changes to *down*, the status of the linked interfaces also changes to *down*.
- When the status of the tracking object changes to *up*, the status of the linked interfaces also changes to *up*.

The device lets you link the following interface types to a tracking object:
- Physical ports
- Link Aggregation interfaces

13.4.1 Special conditions during use

If you manually deactivate the linked interface, then its status remains *down* even if the tracking object status changes to *up*.

The interface status application checks the reason for disabling an interface. If the *Auto-Disable* function has disabled a linked interface, then the interface status application does not enable this port again.

13.4.2 Example for the Interface status application

In the following example, the administrator links the tracking object `if-1` to interface `1/2`. When the status of the tracking object `if-1` changes, the interface status application changes the status of interface `1/2` accordingly. The prerequisite is that for interface `1/1`, a tracking object with *Track name* = `if-1` and *Type* =*`interface`* is set up. See section “Configuring the tracking” on page 298.

Perform the following steps:

- ☐ Open the *Basic Settings > Port* dialog.
  The dialog displays the settings for the individual ports.
  You link a Link Aggregation interface in the *Switching > L2-Redundancy > Link Aggregation* dialog.
- ☐ In the table row for interface `1/2`, *Track name* column, select from the drop-down list the `if-1` tracking object item.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Advanced > Tracking > Applications* dialog to display which applications are linked to the tracking objects.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.

```
track if-status add if-1
```
To link the tracking object `if-1` to interface `1/2`.

```
show track application
```
To check the status of the applications.

```
Type         Track-Id   App-Name                              App-Object-Name
----------   --------   ------------------------------------  --------------
interface           1   IntfState 1/1                         if-1
```

```
save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

14 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 stream on a port (port mirroring)
- Syslog
- Event log
- Cause and action management during selftest

14.1 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 specified in the trap destination table. The device lets you set up the trap destination table with the network management station using SNMP.

14.1.1 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 transferring a configuration file onto 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.

14.1.2 SNMP trap setting

The device lets you send an SNMP trap as a reaction to specific events. Set up 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.
- ☐ Apply 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
- *Network Security > Port Security* dialog
- *Switching > L2-Redundancy > Link Aggregation* dialog
- *Advanced > Tracking > Configuration* 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

14.1.3 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.

14.2 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 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 lets you:
- Out-of-Band signalling using a signal contact
- signal the changed device status by sending an SNMP trap
- detect the device status in the *Basic Settings > System* dialog of the Graphical User Interface
- query the device status in the Command Line Interface

The *Global* tab of the *Diagnostics > Status Configuration > Device Status* dialog lets you set up the device to send a trap to the management station for the following events:
- Incorrect supply voltage
  - at least one of the 2 supply voltages is not operating
  - the internal supply voltage is not operating
- When you operate the device outside of the user-specified temperature threshold values
- Loss of the redundancy (when the device operates in the *Ring Manager* mode)
- The interruption of link connection(s)
  Set up at least one port for this feature. In the table of the *Port* tab, *Propagate connection error* column, you specify for which ports the device will propagate a link interruption to the device status. In the default setting, link connection monitoring is inactive.
- The removal of the external memory (*ENVM*)
  The configuration profile in the external memory (*ENVM*) does not match the settings 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.

14.2.1 Events which can be monitored

Table 39: Device Status events

Name	Meaning
Connection errors	Activate this function to monitor every port link event in which the *Propagate connection error* checkbox is marked.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
Ethernet module removal	Activate this function to monitor the removal of a module. Also activate the individual module to monitor.
External memory removed	Activate this function to monitor the presence of an external storage device.

Table 39: Device Status events (cont.)

Name	Meaning
External memory not in sync with NVM	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (*ENVM*).
Ring redundancy	When ring redundancy is present, activate this function to monitor.
Power supply 1, *Power supply 2*	Activate this function to monitor the power supply.

14.2.2 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, add at least one trap destination that receives SNMP traps.
- ☐ Apply 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.
- ☐ Apply 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 (*ENVM*). 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 (*ENVM*).
`device-status monitor envm-removal`	To monitor the active external memory (*ENVM*). 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 device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. • The device, as a ring participant, has detected an error in its ring redundancy settings.
`device-status monitor temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the value in the *Device status* frame changes to *error*.
`device-status monitor module-removal`	To monitor the modules. When you remove a module from the device, the value in the *Device status* frame changes to *error*.
`device-status module 1`	To monitor module 1. When you remove the module 1 from the device, the value in the *Device status* frame changes to *error*.

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.
- ☐ Apply 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 monitor link-failure`	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`.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`device-status link-alarm`	To monitor the port/interface link. When the link interrupts on a monitored 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.

14.2.3 Displaying the Device Status

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.

`enable`	To change to the Privileged EXEC mode.
`show device-status all`	To display the device status and the setting for the device status determination.

14.3 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

14.3.1 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 40: Security Status events

Name	Meaning
Password default settings unchanged	After installation change the passwords to increase security. When active and the default passwords remain unchanged, the device displays an alarm.
Min. password length shorter than 8	Create passwords more than 8 characters long to maintain a high security posture. When active, the device monitors the *Min. password length* setting.
Password policy settings deactivated	The device monitors the settings located in the *Device Security* > User Management dialog for password policy requirements.
User account password policy check deactivated	The device monitors the settings of the *Policy check* checkbox. When *Policy check* is inactive, the device sends an SNMP trap.
Telnet server active	Activate this function to monitor when the *Telnet* function is active.
HTTP server active	Activate this function to monitor when the *HTTP* function is active.
SNMP unencrypted	Activate this function to monitor when the *SNMPv1* or *SNMPv2* function is active.
Access to System Monitor 1 through the serial interface possible	The device monitors if starting the System Monitor 1 through the serial connection is possible during the system startup.
Saving the configuration profile on the external memory possible	The device monitors the possibility to save settings to the external non-volatile memory (*NVM*).
Link interrupted on enabled device ports	The device monitors the link status of active ports.

Table 40: Security Status events (cont.)

Name	Meaning
Access with HiDiscovery possible	Activate this function to monitor when the HiDiscovery function has write access to the device.
Load unencrypted config from external memory	The device monitors the security settings for loading the configuration from the external NVM.
Self-signed HTTPS certificate present	The device monitors the HTTPS server for self-generated digital certificates.

14.3.2 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, add 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`*.

`security-status monitor http-enabled`	To monitor the HTTP server. When you enable the HTTP server, the value in the *Security status* frame changes to *error*.
`security-status monitor snmp-unsecure`	To monitor the SNMP server. When at least one of the following conditions applies, the value in the *Security status* frame 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* field.
`security-status monitor sysmon-enabled`	To monitor the activation of the *System Monitor 1* function in the device.
`security-status monitor extnvm-upd-enabled`	To monitor the activation of the external non volatile memory update.
`security-status trap`	To send an SNMP trap when the device status changes.

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.
- ☐ Apply 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.
- ☐ Apply 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 `1/1`.

14.3.3 Displaying the Security Status

Perform the following steps:

☐ Open the *Basic Settings > System* dialog.

`enable`	To change to the Privileged EXEC mode.
`show security-status all`	To display the security status and the setting for the security status determination.

14.4 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 you operate the device outside of the user-specified temperature threshold values
- Events for ring redundancy:
  The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve.
  The device, as a ring participant, has detected an error in its ring redundancy settings.
  In the default setting, ring redundancy monitoring is inactive.
- The interruption of link connection(s)
  Set up 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 (*ENVM*)
  The configuration profile in the external memory (*ENVM*) does not match the settings 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.

14.4.1 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.
- ☐ Open the signal contact.
  Select the *open* radio button in the *Configuration* frame.
- ☐ Close the signal contact.
  Select the *close* radio button in the *Configuration* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 mode manual`	To select the manual setting mode for signal contact 1.
`signal-contact 1 state open`	To open signal contact 1.
`signal-contact 1 state closed`	To close signal contact 1.

14.4.2 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.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ In the *Diagnostics > Status Configuration > Alarms (Traps)* dialog, add at least one trap destination that receives SNMP traps.
- ☐ Apply 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.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor temperature`	To monitor the temperature in the device. When the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, the signal contact opens.

`signal-contact 1 monitor ring-redundancy`	To monitor the ring redundancy. The signal contact opens in the following situations: • The device operates as a Redundancy Manager. The redundancy function of the device uses the alternative connection. There is no longer a redundancy reserve. • The device, as a ring participant, has detected an error in its ring redundancy settings.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.
`signal-contact 1 monitor envm-removal`	To monitor the active external memory (*ENVM*). When you remove the active external memory (*ENVM*) from the device, the signal contact opens.
`signal-contact 1 monitor envm-not-in-sync`	To monitor the configuration profiles in the device and in the external memory (*ENVM*). 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 (*ENVM*).
`signal-contact 1 monitor power-supply 1`	To monitor the power supply unit 1. When the device has a detected power supply fault, the signal contact opens.
`signal-contact 1 monitor module-removal 1`	To monitor module 1. When you remove module 1 from the device, the signal contact opens.
`signal-contact 1 trap`	To send an SNMP trap when the status of the operation monitoring changes.
`no signal-contact 1 trap`	To disable the SNMP trap

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.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`signal-contact 1 monitor link-failure`	To monitor the ports/interfaces link. When the link interrupts on a monitored port/interface, the signal contact opens.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`signal-contact 1 link-alarm`	To monitor the port/interface link. When the link interrupts on the port/interface, the signal contact opens.

Events which can be monitored

Table 41: Device Status events

Name	Meaning
Connection errors	Activate this function to monitor every port link event in which the *Propagate connection error* checkbox is marked.
Temperature	Activate this function to monitor if the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value.
Ethernet module removal	Activate this function to monitor the removal of a module. Also activate the individual module to monitor.
External memory removed	Activate this function to monitor the presence of an external storage device.
External memory not in sync with NVM	The device monitors synchronization between the device settings and the configuration profile stored in the external memory (*ENVM*).
Ring redundancy	When ring redundancy is present, activate this function to monitor.
Power supply 1, *Power supply 2*	Activate this function to monitor the power supply.

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 settings for the specified signal contact.

14.5 Port event counter

The port statistics table assists experienced network administrators in identifying potential network interruptions.

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 42: Examples indicating known weaknesses

Counter	Indication of known possible weakness
Received fragments	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium
CRC Error	• Non-functioning controller of the connected device • Electromagnetic interference in the transmission medium • Inoperable component in the network
Collisions	• Non-functioning controller of the connected device • Network over extended/lines too long • Collision or a detected fault with a data packet

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.

14.5.1 Detecting non-matching duplex modes

Potential problems occur when 2 ports directly connected to each other have mismatched duplex modes. These potential problems are difficult to detect. The automatic detection and reporting of this situation has the benefit of recognizing mismatched duplex modes before potential 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 data stream 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:

- 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 43: Evaluation of non-matching of the duplex mode

No.	Automatic configuration	Current duplex mode	Detected error events (≥ 10 after link up)	Duplex modes	Possible causes
5	marked	Full-duplex	None	OK	
6	marked	Full-duplex	Collisions	OK	EMI
7	marked	Full-duplex	Late Collisions	OK	EMI
8	marked	Full-duplex	CRC Error	OK	EMI
13	unmarked	Full-duplex	None	OK	
14	unmarked	Full-duplex	Collisions	OK	EMI
15	unmarked	Full-duplex	Late Collisions	OK	EMI
16	unmarked	Full-duplex	CRC Error	Duplex problem detected	Potential duplex problem, EMI

14.6 Auto-Disable

The device can disable a port on various user-selectable events, such as a detected error or change of condition. Each of these events leads to the shutdown of the port. To recover the port, either clear the condition that caused the port shutdown or specify a timer to automatically re-enable the port.

If the device disables the port, then the device no longer forwards data packets to and from that port. The port LED blinks green 3 times per period and indicates the reason for disabling. In addition, the device generates 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)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (*Port Monitor* function)
- *Link speed/Duplex mode detection* (*Port Monitor* function)

If the interface status application disables the port due to the status of the linked tracking object changes to `down`, then the *Auto-Disable* function does not automatically enable the port.

In the following example, you set up the device to disable a port due to detected violations to the threshold values 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 threshold values specified in the table concur to your preferences for port `1/1`.
- ☐ Open the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- ☐ Enable the *Port Monitor* 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 value 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 set up 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 set up 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 value 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 has expired.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`port-monitor condition crc-fragments count 2000`	To specify the CRC-Fragment counter to 2000 parts per million.
`port-monitor condition crc-fragments interval 15`	To set the measure interval to 15 seconds for CRC-Fragment detection.
`auto-disable timer 120`	To specify the waiting period of `120` seconds, after which the *Auto-disable* function re-enables the port.
`exit`	To change to the Configuration mode.
`auto-disable reason crc-error`	To activate the auto-disable CRC function.
`port-monitor condition crc-fragments mode`	To activate the CRC-Fragments condition to trigger an action.
`port-monitor operation`	To activate the *Port Monitor* function.

When the device disables a port due to threshold value violations, the device lets you use the following commands to manually reset the disabled port.

Perform the following steps:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`auto-disable reset`	To let you enable the port before the time has expired.

14.7 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.

14.8 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 occur.
- receive connection and management information from neighbor 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 end point: 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-capable devices normally block the special Multicast LLDP IEEE MAC address used for information exchange. Non-LLDP-capable 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.

14.8.1 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.

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 MAC address table (forwarding database) contains MAC addresses of devices that the topology table hides for the sake of clarity.

14.8.2 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 DSCP (Differentiated Services Code Point)
- 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 Link Layer Discovery Protocol (LLDP) 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

14.9 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.

14.10 Helping avoid 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.

14.10.1 Helping avoid layer 2 network loops

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 set-up layer 2 network loops.

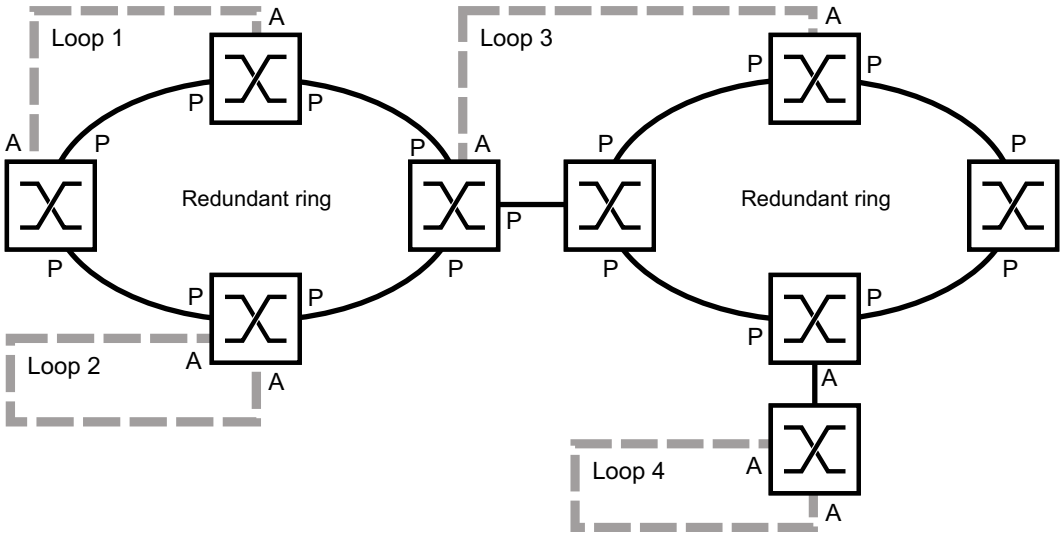


Figure 72: Examples for unintended layer 2 network loops

Assigning 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 that 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`loop-protection tx-interval 5`	To specify the transmit interval, if necessary.
`loop-protection rx-threshold 1`	To specify the receive threshold value, if necessary.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`loop-protection mode active`	To specify the mode `active` for ports that are intended to connect end devices.
`loop-protection mode passive`	To specify the mode `passive` for ports which belong to the redundant rings.
`loop-protection action all`	To specify the action that the device performs when it detects a layer 2 network loop on this port.
`loop-protection operation`	To activate the *Loop Protection* function on the port.
`exit`	To change to the Configuration mode.

Activating 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`loop-protection auto-disable`	To activate the *Auto-Disable* function.

Enabling the Loop Protection function in the device

When finished, enable the *Loop Protection* function in the device.

Perform the following steps:

- ☐ Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`loop-protection operation` — To enable the *Loop Protection* function in the device.

14.10.2 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.

14.11 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:
- ☐ Specifying the sender address
- ☐ Specifying the triggering events
- ☐ Specifying the recipients
- ☐ Specifying the mail server
- ☐ Enabling/Disabling the Email Notification function
- ☐ Sending a test email

14.11.1 Specifying 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 *Email address* field. Add a valid email address.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email from-addr <user@doma.in>`	To change the sender address.

14.11.2 Specifying the triggering events

The device differentiates between the following severities:

Table 44: Meaning of the severities for events

Severity	Meaning
emergency	Device not ready for operation
alert	Immediate user intervention required
critical	Critical status
error	Error status
warning	Warning
notice	Significant, normal status
informational	Informal message
debug	Debug message

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 urgent*
  When an event of the severity assigned or more severe occurs, the device sends an email immediately.
- *Notification non-urgent*
  - 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 urgent* 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 non-urgent* 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.

☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email severity immediate <level>`	To specify the minimum severity for events for which the device sends an email immediately.
`logging email severity periodic <level>`	To specify the minimum severity for events for which the device sends an email periodically.
`logging email subject add <immediate | periodic> TEXT`	To add a subject line with the content `TEXT`.

14.11.3 Changing the sending 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 non-urgent* 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.

☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email duration <30..1440>`	To specify the interval at which the device sends emails with log file.

14.11.4 Specifying 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 *Email address* column, specify the email address of the recipient.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`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`.

14.11.5 Specifying 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.

- ☐ In the *Description* column, enter a meaningful name for the mail server.
- ☐ In the *Active* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	To specify the mail server with the IP address `IP ADDRESS`. The device manages the settings in memory `1..5`.

14.11.6 Enabling/Disabling the Email Notification function

Perform the following steps:

- ☐ Open the *Diagnostics > Email Notification > Global* dialog.
- ☐ Enable the *Email Notification* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email operation`	To enable the sending of emails.
`no logging email operation`	To disable the sending of emails.

14.11.7 Sending 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging email test msgtype <urgent|non-urgent> TEXT`	To send an email with the content `TEXT` to the recipients.

When you do not see any message for detected errors and the recipients obtain the email, the device settings are correct.

14.12 Reports

The following lists reports and buttons available for diagnostics:

- System Log file
  The device logs device-internal events in the System Log file.
- 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 remain available even after powering off the device. 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 number of files set up. 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.

14.12.1 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.
- ☐ Enable the *Console logging* function.
  Select the *On* radio button in the *Console logging* frame.
- ☐ Apply 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.
- ☐ Apply 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 setup 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 to send SNMP Read requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device to send SNMP Write requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Apply 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 IEEE 1686 for Substation Intelligent Electronic Devices.

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ Enable the *CLI logging* function.
  Select the *On* radio button in the *CLI logging* frame.
- ☐ Apply 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 names 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.

14.12.2 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.
- ☐ Enable the *Syslog* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

In the *SNMP logging* frame, set up the following settings for SNMP read and write requests:

Perform the following steps:

- ☐ Open the *Diagnostics > Report > Global* dialog.
- ☐ Enable the *Log SNMP get request* function for the device to send SNMP Read requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Enable the *Log SNMP set request* function for the device to send SNMP Write requests as events to the syslog server.
  Select the *On* radio button in the *SNMP logging* frame.
- ☐ Choose the desired severity level for the get and set requests.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging host add 1 addr 10.0.1.159 severity 3`	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`.
`logging host add 2 addr 2001::1 severity 4`	To add an IPv6 recipient in the syslog servers list. The value `4` means `warning`.
`logging syslog operation`	To enable the *Syslog* function.
`exit`	To change to the Privileged EXEC mode.

```
show logging host                                To display the syslog host settings.
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                        To change to the Configuration mode.
logging snmp-requests get operation              To log the reception of SNMP Get requests.
logging snmp-requests get severity 5             The value 5 specifies the severity level of the event
                                                 that the device logs when it receives an SNMP Get
                                                 request. The value 5 means notice.
logging snmp-requests set operation              To log the reception of SNMP Set requests.
logging snmp-requests set severity 5             The value 5 specifies the severity level of the event
                                                 that the device logs when it receives an SNMP Set
                                                 request. The value 5 means notice.
exit                                             To change to the Privileged EXEC mode.
show logging snmp                                To display the SNMP logging settings.
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.12.3 System Log

The device lets you call up a System Log file of the system events. The table in the *Diagnostics* > Report > *System Log* dialog lists the logged events.

You have the following options:
- View and refresh the System Log file
- Searching for content
- Downloading a copy of the System Log file
- Clearing the System Log file on the device

You have the option to also send the logged events to one or more syslog servers.

View and refresh the System Log file

The device continuously logs events in the System Log file. The display of events in the Graphical User Interface does not update automatically. If the dialog is already open for a while, refresh the display to also display the recently logged events.

Perform the following steps:

- ☐ Refresh the display of the System Log file in the Graphical User Interface. To do this, click the ⟳ button.

```
enable                                           To change to the Privileged EXEC mode.
show logging buffered                            To display the buffered log entries.
```

Searching for content

The device continuously logs events in the System Log file. After a while, the file may contain a large number of events.

Perform the following steps:

- ☐ Look for a keyword in the System Log file. To do this, use the search function of your web browser.

`enable`	To change to the Privileged EXEC mode.
`show logging buffered <filter>`	To display the buffered log entries. You can enter keywords for the severity level, digits, or ranges, separated by a comma. Example: `emergency,alert-error,4,5-6`

Downloading a copy of the System Log file

The device continuously logs events in the System Log file. After a while, the file may contain many events. In the Graphical User Interface, you can download a copy of the System Log file to analyze the logged events on your computer. Using the Command Line Interface, you can save a copy of the System Log file in the external memory (*ENVM*) or on a remote server.

Perform the following steps:

- ☐ Download a copy of the System Log file onto your computer. To do this, click the  button.
- ☐ The web browser saves the file on the computer according to its download settings. If necessary, select the file location.

`enable`	To change to the Privileged EXEC mode.
`copy eventlog buffered envm EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` in the external memory (*ENVM*).
`copy eventlog buffered remote ftp://1.2.3.4/EXAMPLE`	To save a copy of the System Log file with filename `EXAMPLE` on a remote server.

Clearing the System Log file on the device

The device continuously logs events in the System Log file. After a while, the file may contain many events. If you are no longer interested in the logged events, you can clear the System Log file in the device.

Perform the following steps:

- ☐ Delete the content of the System Log file. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`clear logging buffered`	To clear the log file.

14.12.4 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.

When initiating a connection with a syslog server, using a TLS handshake, the device validates the digital certificate received from the server. For this purpose, you transfer the digital certificate from a remote server or from the external memory (*ENVM*) onto the device. Verify that the specified IP address or DNS name of the server matches the `Common Name` or `Subject Alternative Name` information in the digital certificate.

The device sends the TLS encrypted syslog messages over the TCP port specified in the *Destination UDP port* column.

Note:
To establish an encrypted connection using a digital certificate, verify that the `Common Name` or `Subject Alternative Name` information in the digital certificate that you have transferred onto the device matches the IP address or DNS name of the server.

Application example for the Syslog function

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 untrusted networks. To set up a syslog-over-TLS server, transfer the digital certificate onto the device. For security reasons, Hirschmann recommends using only digital certificates signed by a Certification Authority (CA).

Note:
For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the *Syslog* function. See the *Operation* frame.

Perform the following steps:

- ☐ Open the *Diagnostics > Syslog* dialog.
- ☐ Initiate a data connection with the syslog servers.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

The device validates the digital certificate received. The device also authenticates the server and starts sending syslog messages.

- ☐ Transfer the digital certificate from the remote server or from the external memory (*ENVM*) onto the device.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`logging host add 1 addr 192.168.3.215`	To add index `1` to the syslog server with IPv4 address `192.168.3.215`.
`logging host add 2 addr 2001::1`	To add index `2` to the syslog server with IPv6 address `2001::1`.
`logging host modify 1 port 6512 type systemlog`	To specify the port number `6512` and logging the events in the system log.
`logging host modify 1 transport tls`	To specify the type of transmission as *`tls`*.
`logging host modify 1 severity informational`	To specify the type of event to log into the system log as *`informational`*.
`exit`	To change to the Privileged EXEC mode.
`copy syslogcacert evmm`	To transfer the digital certificates from the external memory (*`ENVM`*) onto the device.
`show logging host`	To display the syslog host settings.

14.12.5 Audit Trail

The *Diagnostics > Report > Audit Trail* dialog contains system information and changes to the device settings performed through the Command Line Interface and SNMP. In the case of a change in the device settings, 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 device software update
- Configuration changes using HiDiscovery
- Automatic configuration or device software 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

14.13 Network analysis with TCPdump

Tcpdump is a packet-sniffing UNIX utility used by network administrators to sniff and analyze the data stream on a network. A couple of reasons for sniffing data streams on a network are to verify connectivity between hosts or to analyze the data stream 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.

14.14 Monitoring the data stream with Port Mirroring

The *Port Mirroring* function lets you copy data packets from physical source ports to a physical destination port. Port Mirroring is also known as Switched Port Analyzer (SPAN).

You monitor the data packets 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 effect on the data stream running on the source ports.

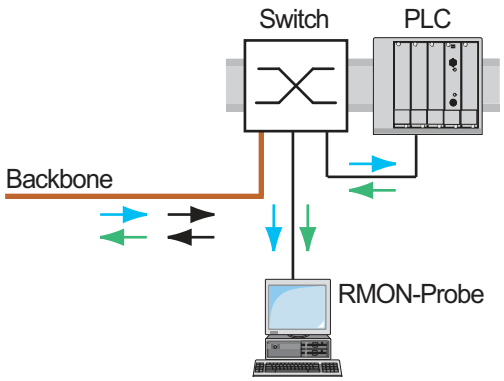


Figure 73: Application example of a port-mirroring setup

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.

14.14.1 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.
- ☐ To access the device management through the destination port:
  In the *Destination port* frame, mark the *Allow management* checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.

To deactivate the *Port Mirroring* function and restore the default settings, click the button.

14.15 Monitoring the data stream with VLAN mirroring

The *VLAN mirroring* function lets you mirror the received data stream that matches a specific VLAN to a selected destination port. The device only copies the data on the VLAN, and sends the original data to the intended recipients. For example, the device can mirror data to a network analyzer connected to the destination port.

Only one of the functions, either the *VLAN mirroring* function or the *Port Mirroring* function, can be active at the same time. When you select VLAN 0 as the source VLAN, the *VLAN mirroring* function is inactive. To disable the *VLAN mirroring* function, unmark the checkbox in the *Enabled* column for the source port.

If the data stream received on the mirrored VLAN exceeds the maximum bandwidth of the destination port, then the device drops some packets to accommodate the maximum bandwidth of the destination port. Even though the device drops some packets, the device continues to mirror packets that match the specified VLAN.

When you specify the PVID on a port as the source VLAN ID, the device mirrors the untagged packets received, but without a VLAN tag. In this case, the device mirrors the packet exactly as it received the packet.

14.15.1 Application example for the VLAN mirroring function

In this application example, Sw 4 mirrors data received on VLAN 20 to a network analyzer on the destination port.

To set up VLAN mirroring on Sw 4, use the following steps:
- ☐ Add the VLAN you want to mirror.
- ☐ Set up VLAN mirroring

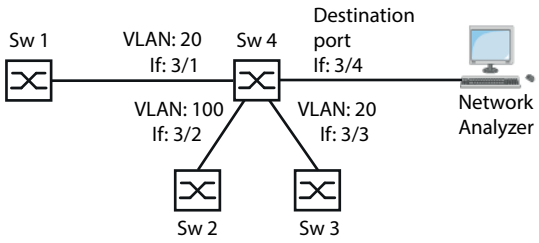


Figure 74: Application example of a VLAN mirroring setup

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the VLAN:
  - ☐ Click the button.
    The dialog displays the *Create* window.
  - ☐ In the *VLAN ID* field, specify the value `20`.
  - ☐ Click the *Ok* button.
  - ☐ In the *Name* column, specify the value `VLAN mirroring port`.
- ☐ Apply the settings temporarily. To do this, click the button.

- ☐ Open the *Diagnostics > Ports > Port Mirroring* dialog.
- ☐ Deactivating the *Port Mirroring* function:
  Unmark every checkbox in the *Enabled* column.
- ☐ Specifying the destination port:
  In the *Destination port* frame, specify the value `3/4`.
- ☐ Specifying the data source:
  In the *VLAN mirroring* frame, *Source VLAN ID* field, specify the value `20`.
- ☐ Enable the *VLAN mirroring* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 20`	To add VLAN `20`.
`name 20 VLAN mirroring port`	To assign the name `20` to the VLAN `VLAN mirroring port`.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`monitor session 1 source vlan 20`	To add VLAN mirroring session `1`, the source is VLAN `20`.
`monitor session 1 destination interface 3/4`	To specify port `3/4` as the destination port.
`monitor session 1 mode`	To activate VLAN mirroring session `1`.

14.16 Monitoring data streams with RSPAN

RSPAN (Remote Switched Port Analyzer) extends the concept of Switched Port Analyzer (SPAN), which is also called Port Mirroring.

In contrast to SPAN, which operates on a single switch device, RSPAN uses a topology of 2 or more RSPAN-enabled devices. This lets you analyze the data stream at a location other than directly at the source.

14.16.1 Purpose

RSPAN lets a network administrator collect data packets from selected locations in a network and monitor the mirrored data packets at a convenient location.

The data packets are collected by one or more devices acting in the *source role*. These so-called *source devices* collect data packets from selectable *source ports* or from a selectable *source VLAN*. A *source device* can have several *source ports* but only one *source VLAN*.

Each RSPAN-enabled device receives and forwards the mirrored data packets on a specified RSPAN VLAN to the final destination. This includes optional devices in an *intermediate role*, so-called *intermediate devices*.

Finally, a device in the *destination role*, a so-called *destination device*, sends the mirrored data packets to its local *destination port*. An analyzer tool, usually a dedicated computer, can then monitor or analyze the mirrored data packets at a convenient, for example, central location.

RSPAN key aspects are:

- Topology
  An RSPAN topology consists of 2 or more RSPAN-enabled devices.
  See “RSPAN topologies” on page 345.
- VLAN
  The RSPAN VLAN transfers the mirrored data packets between RSPAN-enabled devices.
  See “RSPAN VLAN properties” on page 348.
- Roles
  RSPAN roles are specific roles for the devices in an RSPAN topology.
  See “RSPAN device roles” on page 349.
- Uplinks
  RSPAN uplinks can be separate uplinks or shared with normal uplinks.
  See “RSPAN uplinks” on page 351.

14.16.2 RSPAN topologies

RSPAN topologies and the consequential locations of the devices in RSPAN roles can be:

- Line topology
- Tree topology
- Ring topology

Line topology

An RSPAN line topology is a simple line structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, a tree topology.

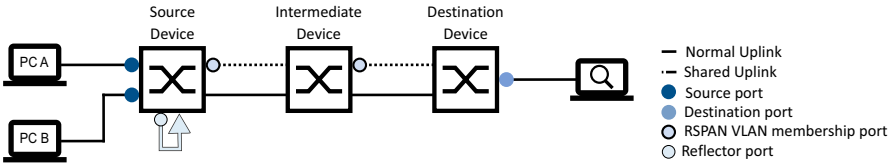


Figure 75: Example of a line topology, using a reflector port (with separate uplinks)

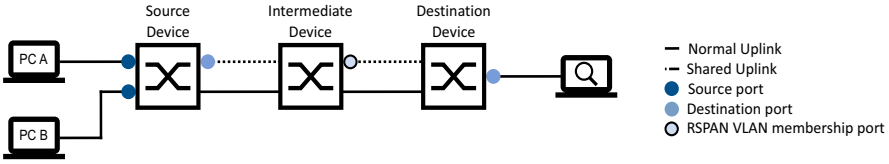


Figure 76: Example of a line topology, without a reflector port (with separate uplinks)

A line topology is a simple topology, where only one *source* and one *destination* device are required, and *intermediate devices* are optional:

- One *source device*
  The *source device* is located at one end of the line, at the data sources to be mirrored.
- One *destination device*
  The *destination device* is located at the other end of the line, near the analyzer tool.
- Optional *intermediate devices*
  The *intermediate devices* are located in the middle of the line, between the *source device* and the *destination device*. You can connect the *source device* directly to the *destination device*, if your situation allows.

The graphics show separate uplinks for RSPAN and non-RSPAN data packets.

You can also create shared uplinks. For this, you use the normal (non-RSPAN) uplinks also for RSPAN. To create shared uplinks, select the existing, non-RSPAN uplink ports as RSPAN ports.

Tree topology

An RSPAN tree topology is a tree structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, a mesh topology.

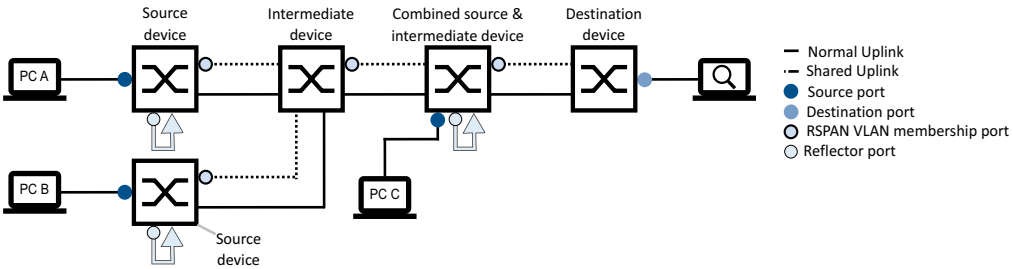


Figure 77: Example of a complex tree topology, using reflector ports (with separate uplinks)

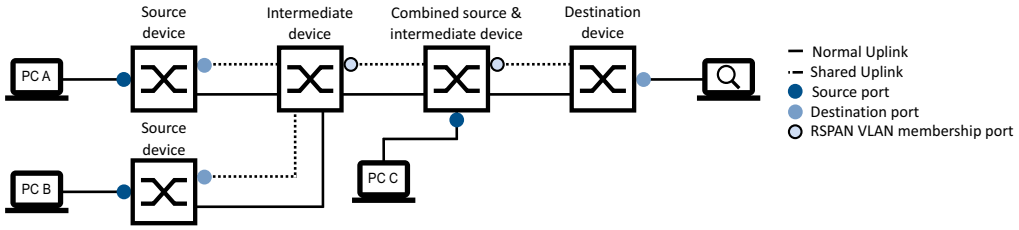


Figure 78: Example of a complex tree topology, without reflector ports (with separate uplinks)

A tree topology consists of:

- 2 or more *source devices*
  The *source devices* are located at the leaves of the tree, at the data sources to be mirrored.
- One *destination device*
  The *destination device* is located at the root of the tree, near the analyzer tool.
- Optional *intermediate devices*
  The *intermediate devices are* located as nodes in the middle of the tree, between the *source device* and the *destination device*. You can connect the *source devices* directly to the *destination device*, if your situation allows.

Tree topology subtypes:

- Simple tree topology:
  A simple tree topology requires only one *destination* and several *source devices*. *Intermediate* devices are optional, and the topology requires no *combined source/intermediate devices*.
- Complex tree topology:
  A complex tree topology requires additionally one or more *combined source/intermediate devices*. See “Combined source/intermediate role” on page 350.

The graphics show separate uplinks for RSPAN and non-RSPAN data packets.

You can also create shared uplinks. For this, you use the normal (non-RSPAN) uplinks also for RSPAN. To create shared uplinks, select the existing, non-RSPAN uplink ports as RSPAN ports.

Ring topology

An RSPAN ring topology is a ring structure, superimposed on the existing network. The underlying network may have a more generalized topology, for example, coupled rings.

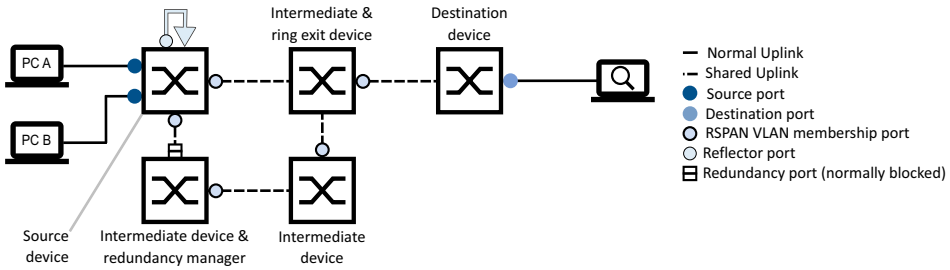


Figure 79: Example of a simple ring topology based on an existing redundant ring (with shared links)

A ring topology consists of:
- In the ring:
  - One *source device*
    The *source device* is located in the ring, at the data sources to be mirrored.
    The *source device* has 2 *destination ports* and needs a *reflector port*.
  - One or more *intermediate devices*
    One of the *intermediate devices* forwards the RSPAN data packets out of the ring. In the following, this device is called the ring exit device.
    The other *intermediate devices* are located in the ring, between the *source device* and the ring exit device.
    The *intermediate devices* have one RSPAN VLAN membership port each.
- Outside the ring:
  - One *destination device*
    The *destination device is* located outside the ring, near the analyzer tool.
    You can connect the ring exit device directly to the *destination device*, if your situation allows.
  - Optional *intermediate devices*
    These optional *intermediate devices* connect the ring exit device to the *destination device*.

When setting up the RSPAN VLAN membership ports of the *intermediate devices* in the ring, consider the following data packet stream scenarios to the ring exit device:
- The regular RSPAN data packet stream, with the ring intact and the redundancy port blocked
- The alternate RSPAN data packet stream, with the ring interrupted and the redundancy port active

Note:
The special case where the *source device* is also the ring exit device, is considered a line topology.

Ring topology subtypes:
- Simple ring topology
  A simple ring topology requires only *source, intermediate*, and *destination* devices, but no *combined source/intermediate devices*.
- Complex ring topology
  A complex ring topology additionally requires one or more *combined source/intermediate devices*. See “Combined source/intermediate role” on page 350.

14.16.3 RSPAN VLAN properties

The flow of mirrored data packets within the RSPAN VLAN is unidirectional towards the *destination port* of the *destination device*. Consequently, the devices disable source MAC address learning in the RSPAN VLAN and flood the mirrored data packets within the RSPAN VLAN. Because of this, only the RSPAN *destination ports* have to be set up as a members of the RSPAN VLAN.

In contrast, ports receiving RSPAN data packets are not members of the RSPAN VLAN.

The *destination ports* of a *source device* send RSPAN data packets in the following way:
- The device adds a single RSPAN VLAN tag to untagged source data packets.
- The device inserts an additional RSPAN VLAN tag into tagged source data packets. This results in double VLAN tagged data packets. The device inserts the RSPAN VLAN tag as the first VLAN tag (outer tag, EtherType 0x8100).

14.16.4 RSPAN device roles

The possible RSPAN roles in a topology have the following names, instances, functions, and specific settings:
- Destination role
- Source role
- Intermediate role
- Combined source/intermediate role

Destination role

The *destination role* is mandatory and requires exactly one instance in an RSPAN topology.
- A *destination device* has its *destination port* connected to an analyzer tool.
- In a tree topology, the *destination device* is the root of the tree.
- In a redundant ring, place the *destination device* outside the ring. This makes the setup of the *destination device* easier. See “Use of underlying redundancy protocols” on page 352.

The *destination device* receives the mirrored data packets on the RSPAN VLAN, either directly from the *source devices*, or indirectly through *intermediate devices*.

The *destination port* has the following properties:
- On a *destination device*, you can set up exactly one *destination port*.
- The *destination port* usually keeps the RSPAN VLAN tag when sending a data packet to the analyzer tool.
- If desired, the *destination port* can also strip the RSPAN VLAN tag.
  - For a tagged source data packet, this restores the original VLAN tag.
  - For an untagged source data packet, this restores the original untagged data packet.

Source role

The *source role* is mandatory and needs one or more instances in an RSPAN topology. A *source device* only collects data packets from *source ports* or a *source VLAN*. A pure *source device* has no ports that receive RSPAN data packets from other devices. For a *combined source/intermediate device*, see “Combined source/intermediate role” on page 350.

The *source device* collects the data packets it receives or sends on its selected local *source ports* or its selected *source VLAN*. The device forwards the mirrored data packets on the RSPAN VLAN, either directly to the *destination device*, or to an *intermediate device*.
- The *source device* supports one *destination port* without the need for a *reflector port*.
- To set up a *source device* with 2 *destination port*s, set up a *reflector port*. A possible use case is a *source device* in a ring redundancy topology. See “Use of underlying redundancy protocols” on page 352.
- The *destination port* adds the RSPAN VLAN tag when sending the data packet.

Note:
If you do not use a *reflector port*, the device automatically adds an RSPAN VLAN tag to the source data packets regardless of the *destination port’s* tag setting `T` (tagged) or `U` (untagged). Therefore, you do not need to set up this *destination port* as a RSPAN VLAN member.

Intermediate role

Depending on the RSPAN topology, the *intermediate role* has the following number of instances:

Table 45: Intermediate role instances, by topology

Topology	Subtype	Intermediate role instances
Line	-	optional
Tree	simple	optional
	complex	optional
Ring	simple	one or more
	complex	one or more

For an *intermediate device*, you only need to set up the RSPAN VLAN. The device does not need any specific RSPAN settings.

An *intermediate device* has one or more ports that receive RSPAN data packets but neither *source ports* nor a *source VLAN*.

An *intermediate device* receives the mirrored data packets on the RSPAN VLAN and forwards the mirrored data packets. When sending the data packets, the *destination port* keeps the RSPAN VLAN tag.

Note:
Verify that the ports receiving the mirrored data packets are not members of the RSPAN VLAN.

Combined source/intermediate role

Depending on the RSPAN topology, the *combined source/intermediate device* has the following number of instances:

Table 46: Combined source/intermediate role instances, by topology

Topology	Subtype	Combined source/intermediate role instances
Line	-	-
Tree	simple	none
	complex	one or more
Ring	simple	none
	complex	one or more

A *combined source/intermediate device* integrates the functions of a *source device* with that of an *intermediate device*:

- The *combined source/intermediate device* is located at the nodes of the topology tree, like *intermediate devices*.
- The device collects the data packets it receives or sends on its selected local *source ports* or a selected *source VLAN*.
- The device forwards the mirrored data packets, either directly to the *destination device*, or to another *intermediate device* towards the *destination device*. When sending the data packets, the *destination port* adds the RSPAN VLAN tag to the source data packets.
- The device additionally receives mirrored data packets on one or more additional ports, either directly from one or more *source devices*, or from one or more other *intermediate devices*.
- The device forwards the mirrored data packets, either directly to the *destination device*, or to another *intermediate device* towards the *destination device*. When sending the data packets, the *destination port* keeps the RSPAN VLAN tag in the received mirrored data packets.

- The device requires specific *source device* settings in addition to the RSPAN VLAN settings of an *intermediate device*.
- The device supports one *destination port* without the need for a *reflector port*.
- To set up the device with 2 *destination ports*, use a *reflector port*. A possible use case is a *source device* in a ring redundancy topology. See “Use of underlying redundancy protocols” on page 352.

Note:
Due to the nature of a *combined source/intermediate device*, you need to set up the RSPAN VLAN membership of the *destination port* even if you do not use a *reflector port*.

14.16.5 RSPAN uplinks

For a shared RSPAN uplink, the *source device* or *intermediate device* send the mirrored data packets over an existing, normal uplink.

- You do not need to connect an additional cable.
- A shared uplink is necessary if you want to use the device as a *source device* or *intermediate device* in a ring redundancy topology.
- If the combined data rate of the RSPAN and non-RSPAN data packets exceeds the bandwidth of the shared uplink, RSPAN data packets and non-RSPAN data packets may affect each other. See “Packet prioritization” on page 353.

For a separate RSPAN uplink, the *source device* or *intermediate device* send the mirrored data packets over a separate connection different from the existing uplink.

- This requires an extra cable connection.
- A separate RSPAN uplink provides an exclusive path for RSPAN data packets. Consequently, the non-RSPAN data packets on their uplink are unaffected by the RSPAN data packets on the separate uplink.

For both uplink types, the RSPAN ports may require individual *Spanning Tree* settings. See “Use of underlying redundancy protocols” on page 352.

14.16.6 Reflector port on a source device

The *reflector port* in a *source device* has a special function without a physical connection. The *reflector port* internally receives the mirrored data packets and reflects (mirrors) them into the RSPAN VLAN instead of sending them. This way, the *reflector port* transforms the function of local Switched Port Analyzer (SPAN), or *Port Mirroring*, into the remote function, RSPAN.

A *source device* supports a *reflector port* for one or more *destination ports* as well as one *destination port* without the need for a *reflector port*.

You use a *reflector port* to set up a *source device* with 2 *destination port*s. A possible use case is a *source device* in a ring redundancy topology. See “Use of underlying redundancy protocols” on page 352.

Note:
A setup, where the reflector port has a link, is unsupported.

14.16.7 Use of underlying redundancy protocols

You can use RSPAN in combination with the following redundancy protocols:
- Ring redundancy
- Link Aggregation
- Spanning Tree

Ring redundancy

RSPAN-enabled devices can forward RSPAN data packets over an underlying ring redundancy topology. Each ring connection serves as an RSPAN uplink between the *source device* and the directly connected *intermediate devices*, as well as between the other *intermediate devices*. This creates a redundant, shared RSPAN uplink.

A ring topology requires shared uplinks. The participating devices transmit the RSPAN data packets together with the other packets over their ring ports.

Note:
The RSPAN roles are independent of the ring redundancy roles like *ring switch* and *ring manager*. However, there are recommendations which of the ring redundancy participants are best used as an *RSPAN source device*.

Planning RSPAN device roles and their setup in a redundant ring:
- ☐ Place the *destination device* outside the ring.
  This makes the setup of the *destination device* easier.
- ☐ If possible, use the one of the following *ring redundancy devices* as the RSPAN *source device*:
  - The *ring manager*
  - The *ring switch* connected to the blocked port of the *ring manager*

  This minimizes the flooding of mirrored data packets into paths not leading to the ring exit device, because the *ring manager* blocks one of these paths in the regular case.
- ☐ If you cannot use one of the above mentioned ring redundancy devices as the *source device*, flooding of mirrored data packets into paths not leading to the ring exit device is inevitable. Weigh up the advantages and disadvantages for your specific use case.
- ☐ If you plan a complex ring topology, you will need at least one *combined source/intermediate device* in addition to the *source device*. The same recommendations apply as for the simple ring topology which ring participants are best used as *source devices* or *combined source/ intermediate devices*.
- ☐ On the *source device*, set up both ring ports as *destination ports*.
  Use a *reflector port*.
- ☐ On the *intermediate devices* in the ring:
  - Determine the device that sends the mirrored data packets out of the ring.
    In the following, this device is called the ring exit device.
  - For the ring exit device, set up the port leading out of the ring as an RSPAN VLAN member.
  - For the other *intermediate devices* on the path to the ring exit device, set up the ring ports connected to the next *intermediate device* or the ring exit device as an RSPAN VLAN member. Consider both data packet stream scenarios: with the ring intact and with the ring interrupted.

Link Aggregation

On the *source device*:
- If you set up a *reflector port*, the device can forward RSPAN data packets over a *Link Aggregation Group* (*LAG*).
- On a *source device* without a *reflector port*, the *destination port* needs to be a physical port.

The *destination port* of the *destination device* needs to be a physical port.

Spanning Tree

For shared RSPAN uplinks based on a mesh topology with *Spanning Tree* (*STP*, *RSTP*, or *MSTP*), RSPAN requires no further *Spanning Tree* settings.

If you use separate RSPAN uplinks, deactivate the *Spanning Tree* function on the ports for the separate RSPAN uplinks.

For shared RSPAN uplinks based on a mesh topology with *MSTP*: Verify that the RSPAN topology matches the underlying *MSTP* topology for the RSPAN VLAN ID.

If you want RSPAN to use the redundant paths provided by *Spanning Tree*, consider setting up a RSPAN topology similar to a ring topology. This means:
- The *source device* may require 2 or more *destination ports* and then require a *reflector port*.
- The *intermediate devices* may require 2 or more RSPAN VLAN membership ports.

In the above case, the use of redundant RSPAN paths will result in the mirrored data packets being flooded into paths that lead to the *destination device*, but these paths are blocked by the redundancy protocol in the regular case. Weigh up the advantages and disadvantages for your specific use case.

14.16.8 Packet prioritization

The *source device* sends the mirrored data packets with the fixed *CoS priority* of `0 (best effort)` in the VLAN tag.

If the combined data rate of the RSPAN and non-RSPAN data packets exceeds the bandwidth of the shared uplink, RSPAN data packets and non-RSPAN data packets may affect each other.

If you cannot tolerate a loss of non-RSPAN data packets and cannot solve this situation by other means, consider VLAN-tagging your non-RSPAN data packets and assign a *CoS priority* of `2 (excellent effort)` or higher to minimize the impact of RSPAN data packets on non-RSPAN data packets.

14.16.9 Starting point for the examples

The network administrator wants to monitor specific data packets using a network analyzer tool located at a central location in the network. The options for setting up RSPAN devices in an existing network are illustrated below.

Boundary conditions:
- Device 1 collects the data packets from PC 1 on port 1/2.
- The analyzer tool, which data accepts packets with a single or a double VLAN tag, is connected to device 3, port 3/3.
- The devices 1 and 3 are connected by device 2. The RSPAN topology therefore is a simple line.
- For a possible separate uplink, the devices 1, 2 and 3 have unused ports available and a physical network connection is available between the devices 1 and 2, as well between the devices 2 and 3.
- The devices in the RSPAN topology are RSPAN-capable.

Setup options chosen by the network administrator:
- Separate or shared RSPAN uplinks are both possible and will be decided later.
- The RSPAN VLAN ID for the examples is 30.
- Use PC 2 to set up RSPAN in the devices.

RSPAN data rate and connection bandwidth:
- For separate RSPAN uplinks:
  - Depending on the data rate of the RSPAN data packets and the bandwidth of the RSPAN connections, the device may drop some RSPAN data packets.
- For shared RSPAN uplinks:
  - Depending on the combined data rate of RSPAN and non-RSPAN data packets and the bandwidth of the shared connections, RSPAN and non-RSPAN data packets may affect one another.
- To address this, use connections with sufficient bandwidth, for example, Gigabit ports, LAG interfaces, or a combination thereof.

Note:
If you set up a *source device* without a *reflector port*, the *destination port* of the *source device* needs to be a physical port.

14.16.10 Example: RSPAN with a reflector port

In the following example, you set up a simple RSPAN line topology, using a *reflector port* on the *source device*. There are 2 options, either with separate or with shared uplinks.

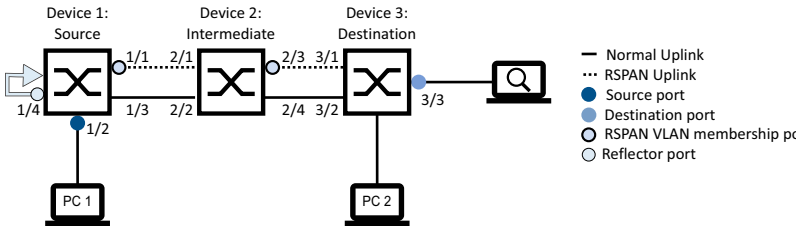


Figure 80: RSPAN in a line topology, using a reflector port (with separate uplinks)

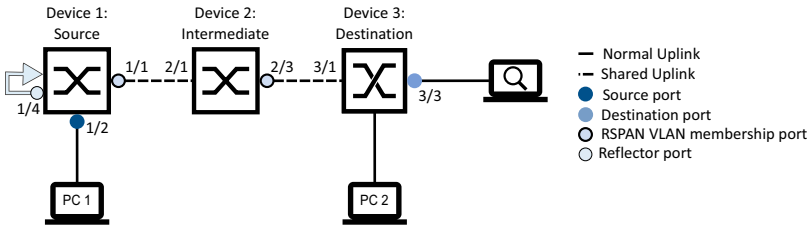


Figure 81: RSPAN in a line topology, using a reflector port (with shared uplinks)

The work steps are the same for both options. The only difference is which ports make up the existing uplink for non-RSPAN packets.

- For a separate uplink, the existing uplink for non-RSPAN packets connects ports 1/3 and 2/2 and ports 2/4 and 3/2 respectively. The work steps will create a separate uplink for RSPAN packets after you physically connect the respective RSPAN ports.
- For a shared uplink, the existing uplink for non-RSPAN packets connects ports 1/1 and 2/1 and ports 2/3 and 3/1 respectively. The work steps will then create a shared uplink for RSPAN packets and non-RSPAN packets.

Setting up device 1 as the source device

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - Click the button.
    The dialog displays the *Create* window.
  - In the *VLAN ID* field, specify the value `30`.
  - Click the *Ok* button.
  - In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Specify the port connected to the *intermediate device*.
  In the VLAN `30` table row, column of port `1/1`, select the `T` item from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > RSPAN* dialog.
- ☐ Specify the *source role*.
  In the *Role* frame, select the *Source switch* item from the drop-down list.
- ☐ Specify the reflector port.
  In the *Reflector port* frame, select port `1/4` from the *Reflector port* drop-down list.
- ☐ Specify the RSPAN VLAN ID.
  In the *RSPAN* frame, *RSPAN Destination VLAN ID* field, specify the value `30`.
- ☐ Specify the *Source port*.
  In the row of port `1/2`, *Active* column, mark the checkbox.
- ☐ Specify the type of the data packets to be mirrored.
  In the row of port `1/2`, *Type* column, select the `txrx` item from the drop-down list.
- ☐ Enable the function.
  In the *Operation* frame, select the `On` radio button.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of the *destination port*, interface `1/1`.
`vlan participation include 30`	To add port `1/1` to the RSPAN VLAN `30`.
`vlan tagging 30`	To send tagged data packets for the RSPAN VLAN `30`.
`exit`	To change to the Configuration mode.
`monitor session 1 source interface 1/2 operation enable`	To add port `1/2` as a *source port* to session `1`.
`monitor session 1 source interface 1/2 direction txrx`	To specify the type of the data packets to be mirrored on port `1/2` as `txrx` in session `1`.
`monitor session 1 remote-vlan 30 reflector-port 1/4`	To add VLAN `30` as the RSPAN VLAN, and to add port `1/4` as the *reflector port* to session `1`.
`monitor session 1 mode enable`	To activate the remote port mirroring session `1`.
`exit`	To change to the Privileged EXEC mode.

Setting up device 2 as the intermediate device

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - – Click the button.
    The dialog displays the *Create* window.
  - – In the *VLAN ID* field, specify the value `30`.
  - – Click the *Ok* button.
  - – In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Specify the port connected to the *destination device*.
  In the VLAN `30` table row, column of port `2/3`, select the `T` item from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 2/3`	To change to the Interface Configuration mode of the *destination port*, interface `2/3`.

`vlan participation include 30`	To add port `2/3` to the RSPAN VLAN `30`.
`vlan tagging 30`	To send tagged data packets for the RSPAN VLAN `30`.
`exit`	To change to the Configuration mode.

Setting up device 3 as the destination device

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - Click the button.
    The dialog displays the *Create* window.
  - In the *VLAN ID* field, specify the value `30`.
  - Click the *Ok* button.
  - In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > RSPAN* dialog.
- ☐ Specify the *destination role*.
  In the *Role* frame, select the *Destination switch* item from the drop-down list.
- ☐ Specify the RSPAN VLAN.
  In the *RSPAN* frame, *RSPAN Source VLAN ID* field, specify the value `30`.
- ☐ Specify the *destination port*.
  In the *Destination port* frame, select port `3/3` from the *Destination port* drop-down list.
- ☐ Enable the function.
  In the *Operation* frame, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`monitor session 1 destination interface 3/3`	To add port `3/3` as the *destination port* to session `1`.
`monitor session 1 source remote-vlan 30`	To add VLAN `30` as the RSPAN VLAN to session `1`.
`monitor session 1 mode enable`	To activate the remote port mirroring session `1`.
`exit`	To change to the Privileged EXEC mode.

14.16.11 Example: RSPAN without a reflector port

In the following example, you set up a simple RSPAN line topology, without a *reflector port* on the *source device*. There are 2 options, either with separate or with shared uplinks.

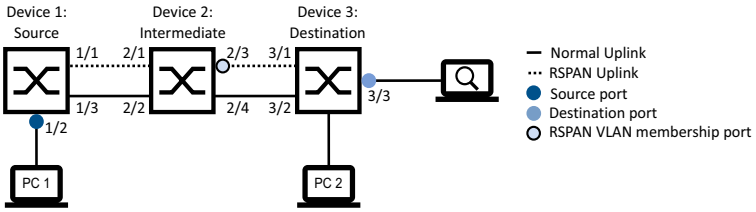


Figure 82: RSPAN in a line topology, without a reflector port (with separate uplinks)

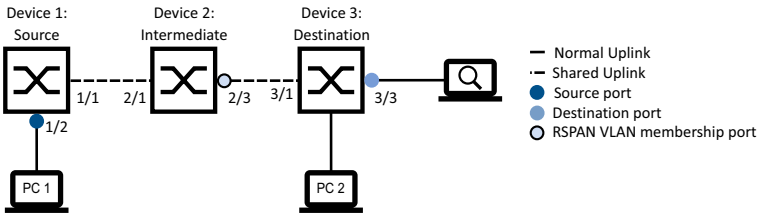


Figure 83: RSPAN in a line topology, without a reflector port (with shared uplinks)

The work steps are the same for both options. The only difference is which ports make up the existing uplink for non-RSPAN packets.

- For a separate uplink, the existing uplink for non-RSPAN packets connects ports 1/3 and 2/2 and ports 2/4 and 3/2 respectively. The work steps will create a separate uplink for RSPAN packets after you physically connect the respective RSPAN ports.
- For a shared uplink, the existing uplink for non-RSPAN packets connects ports 1/1 and 2/1 and ports 2/3 and 3/1 respectively. The work steps will then create a shared uplink for RSPAN packets and non-RSPAN packets.

Setting up device 1 as the source device

Perform the following steps:

- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - Click the button.
    The dialog displays the *Create* window.
  - In the *VLAN ID* field, specify the value `30`.
  - Click the *Ok* button.
  - In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Ports > RSPAN* dialog.
- ☐ Specify the *source role*.
  In the *Role* frame, select the *Source switch* item from the drop-down list.
- ☐ Specify the RSPAN VLAN ID.
  In the *RSPAN* frame, *RSPAN Destination VLAN ID* field, specify the value `30`.

- ☐ Specify the *Source port*.
  In the row of port `1/2`, *Active* column, mark the checkbox.
- ☐ Specify the type of the data packets to be mirrored.
  In the row of port `1/2`, *Type* column, select the `txrx` item from the drop-down list.
- ☐ Specify the *destination port*.
  In the *Destination port* frame, select port `1/1` from the *Destination port* drop-down list.
- ☐ Enable the function.
  In the *Operation* frame, select the `On` radio button.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`monitor session 1 source interface 1/2 operation enable`	To add port `1/2` as a *source port* to session `1`.
`monitor session 1 source interface 1/2 direction txrx`	To specify the type of the data packets to be mirrored on port `1/2` as `txrx` in session `1`.
`monitor session 1 remote-vlan 30`	To use VLAN `30` as the RSPAN VLAN in session `1`.
`monitor session 1 remote-vlan 30 destination port 1/1`	To add VLAN `30` as the RSPAN VLAN, and to add port `1/1` as the *destination port* to session `1`.
`monitor session 1 mode enable`	To activate the remote port mirroring session `1`.

Setting up device 2 as the intermediate device

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - – Click the button.
    The dialog displays the *Create* window.
  - – In the *VLAN ID* field, specify the value `30`.
  - – Click the *Ok* button.
  - – In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Specify the port connected to the *destination device*.
  In the VLAN `30` table row, column of port `2/3`, select the `T` item from the drop-down list.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.

`configure`	To change to the Configuration mode.
`interface 2/3`	To change to the Interface Configuration mode of the *destination port*, interface `2/3`.
`vlan participation include 30`	To add port `2/3` to the RSPAN VLAN `30`.
`vlan tagging 30`	To send tagged data packets for the RSPAN VLAN `30`.
`exit`	To change to the Configuration mode.

Setting up device 3 as the destination device

Perform the following steps:

- ☐ Open the *Switching* > *VLAN* > *Configuration* dialog.
- ☐ Add the RSPAN VLAN:
  - Click the button.
    The dialog displays the *Create* window.
  - In the *VLAN ID* field, specify the value `30`.
  - Click the *Ok* button.
  - In the VLAN `30` table row, *RSPAN VLAN* column, mark the checkbox.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Diagnostics* > *Ports* > *RSPAN* dialog.
- ☐ Specify the *destination role*.
  In the *Role* frame, select the *Destination switch* item from the drop-down list.
- ☐ Specify the RSPAN VLAN.
  In the *RSPAN* frame, *RSPAN Source VLAN ID* field, specify the value `30`.
- ☐ Specify the *destination port*.
  In the *Destination port* frame, select port `3/3` from the *Destination port* drop-down list.
- ☐ Enable the function.
  In the *Operation* frame, select the *On* radio button.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`vlan add 30`	To add VLAN `30`.
`remote-vlan 30`	To specify VLAN `30` as the RSPAN VLAN ID.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`monitor session 1 destination interface 3/3`	To add port `3/3` as the *destination port* to session `1`.
`monitor session 1 source remote-vlan 30`	To add VLAN `30` as the RSPAN VLAN to session `1`.
`monitor session 1 mode enable`	To activate the remote port mirroring session `1`.

14.17 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

Set up 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`selftest action task log-only`	To send a message to the event log when a task is unsuccessful.
`selftest action resource send-trap`	To send an SNMP trap when there are insufficient resources.
`selftest action software send-trap`	To send an SNMP trap when the software integrity has been lost.
`selftest action hardware reboot`	To reboot the device when hardware degradation occurs.

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 self-test during a cold start.

- *SysMon1 is available* checkbox
  Activates/deactivates the option to start the System Monitor 1 during system startup.
  - `marked` (default setting)
    During system startup, the boot menu will display the System Monitor 1 item. The prerequisite is that the management station is connected to the device through the serial connection.
    To actually start the System Monitor 1, select this item during system startup, see section "System Monitor 1" on page 39.
  - `unmarked`
    During system startup, the boot menu will not display the System Monitor 1 item.
    No one can start the System Monitor 1.
- *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:

`selftest ramtest`	To activate RAM self-test on cold start.
`no selftest ramtest`	To deactivate RAM self-test.
`selftest system-monitor`	To activate the option to start the System Monitor 1. During system startup, the boot menu will display the System Monitor 1 item.
`no selftest system-monitor`	To deactivate the option to start the System Monitor 1. During system startup, the boot menu will not display the System Monitor 1 item.
`show selftest action`	To display the actions to be taken in the event of device degradation.

```
Cause     Action
--------- ----------
task      reboot
resource  reboot
software  reboot
hardware  reboot
```

`show selftest settings` — To display the selftest settings.

```
Selftest settings
-----------------
Test RAM on cold start.....................enabled
System Monitor 1...........................enabled
Boot default configuration on error.........enabled
```

14.18 Copper cable test

Use this function to check a copper cable attached to a port for a short or open circuit. The test interrupts the data stream, 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*
  Indicates a short circuit in the cable or the port is inactive
- *unknown*
  Indicates an untested cable or an unplugged cable

14.19 Network monitoring with sFlow

SFlow is a standard protocol for monitoring networks. The device provides this function for visibility into network activity, enabling effective management and control of network resources.

The *SFlow* monitoring system consists of an *SFlow* agent, embedded in the device and a central *SFlow* collector. The agent uses sampling technology to capture the data packet statistics. *SFlow* instances associated with individual data sources within the agent perform packet flow and counter sampling. Using *SFlow* datagrams the agent forwards the sampled data packet statistics to an *SFlow* collector for analysis.

The agent uses 2 forms of sampling, a statistical packet based sampling of packet flows and a timed based sampling of counters. An *SFlow* datagram contains both types of samples. Packet flow sampling, based on a sampling rate, sends a steady, but random stream of datagrams to the collector. For time-based sampling, the agent polls the counters at set intervals to fill the datagrams.

The device implements datagram version 5 for the *SFlow* agent.

The user-defined *SFlow* functions are:

- Sampler configuration, packet flow sampling:
  - data source port number, to sample physical ports
  - receiver index associated with the sampler
  - Sampling rate
    The device counts the packets of received data. When the count reaches the user-defined number, the agent samples the packet.
    Range: `256..65535`
    `0` = function inactive
  - Header size in bytes to sample
    Range: `20..256`
- Poller configuration, counter sampling:
  - data source port number, available for physical ports
  - receiver index associated with the poller
  - Interval, in seconds, between samples
    Range: `0..86400 (1 d)`
- Receiver configuration, up to 8 entries:
  - Owner name, to claim an *SFlow* entry
  - timeout, in seconds, until sampling is stopped and the device releases the receiver along with the sampler and the poller
  - datagram size
  - IP address
  - port number

To set up the *SFlow* agent for a monitoring session, first set up an available receiver. Then, set up a sampling rate to perform packet flow sampling. Additionally, set up a polling interval for counter sampling.

For example, Company XYZ wishes to monitor data flow on a device. The IP address for the remote server containing the sFlow collector, is `10.10.10.10`. XYZ requires a sample of the first 256 bytes of every 300th packet. Furthermore, XYZ requires counter polling every 400 s.

Perform the following steps:

- ☐ Open the *Diagnostics > SFlow > Receiver* dialog.
- ☐ For the name of the person or organization controlling the receiver, enter the value `XYZ` in the *Name* column.
- ☐ For the remote server IP address, on which the *SFlow* collector software runs, specify the value `10.10.10.10` in the *IP address* column.
- ☐ Open the *Diagnostics > SFlow > Configuration* dialog, *Sampler* tab.
- ☐ In the *Receiver* column, select the index number of the receiver specified in the previous steps.
- ☐ In the *Sampling rate* column, specify the value `300`.
- ☐ In the *Max. header size [byte]* column, specify the value `256`.
- ☐ Open the *Diagnostics > SFlow > Configuration* dialog, *Poller* tab.
- ☐ In the *Receiver* column, select the index number of the receiver specified in the previous steps.
- ☐ In the *Interval [s]* column, specify the value `400`.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`sflow receiver 1 owner XYZ ip 10.10.10.10`	To set up an *SFlow* receiver
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`sflow sampler receiver 1 rate 300`	To assign the *SFlow* sampler on the port to the previously specified receiver with a sampling rate of `300`.
`sflow sampler maxheadersize 256`	To set up the maximum header size of the *SFlow* sampler to the value `256`.
`sflow poller receiver 1interval 400`	To assign the *SFlow* poller to the previously specified receiver and to sample data for `400` s.

15 Advanced functions of the device

15.1 DHCP server

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). This reduces the effort required for manual setup. The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The procedure for assigning the IP settings consists of 4 phases:
- *DISCOVER* sent by the DHCP client
- *OFFER* sent by the DHCP server
- *REQUEST* sent by the DHCP client
- *ACKNOWLEDGE* sent by the DHCP server

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The device lets you activate the *DHCP Server* function globally or on single physical ports.

15.1.1 Settings that the server assigns to the clients

When operating as a DHCP server, the device assigns the IP settings to the client devices based on the following parameters:
- MAC address of the client device
- Physical port to which the client device is connected
- VLAN of which the client device is a member

The device assigns the following IP settings to the client devices:
- IP address
- Subnet mask
- Default gateway, if specified
- Further network settings, if specified

15.1.2 Pools

The device stores the IP settings in two types of pools.
- Static pools
  To assign the same IP address to a specific device each time, the device stores the relevant IP settings in a pool whose address range is exactly one IP address.
  Static pools are useful, for example, to assign a fixed IP address to a server, NAS, or printer.
- Dynamic pools
  To assign IP addresses from a certain address range, the device stores the relevant IP settings in a pool whose address range includes multiple IP addresses.
  Dynamic pools are useful, for example, to assign a certain IP address to client devices that belong to a certain VLAN.

Setting up a static pool

In the following example, you set up the device to assign IP settings from a certain static pool to a certain client device connected to a certain port.

The static pool is to be set up based on the following parameters:
- MAC address of the client device: `ec:e5:55:d6:50:01`
- Physical port to which the client device is connected on the server device: `1/1`
- IP address that the device should assign to the client device: `192.168.23.42`
- The assigned IP settings are valid for 2 days: `172800`

Perform the following steps:

- ☐ Open the *Advanced > DHCP > DHCP Server > Pool* dialog.
- ☐ Add a table row. To do this, click the button.
- ☐ Specify the following settings for the table row:
  - *IP range start* column = `192.168.23.42`
  - *Port* column = `1/1`
  - *MAC address* column = `ec:e5:55:d6:50:01`
  - *Lease time [s]* column = `172800`
  - *Active* column = marked
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Advanced > DHCP > DHCP Server > Global* dialog.
- ☐ Verify that the DHCP function is active on port `1/1`.
  If not already done, mark the checkbox in the *DHCP server active* column for port `1/1`.
- ☐ Enable the DHCP server globally.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 1 static 192.168.23.42`	To add a static pool with index `1` with the IP address `192.168.23.42`.
`dhcp-server pool modify 1 mode interface 1/1`	To assign the static pool with index `1` to physical port `1/1`.
`dhcp-server pool modify 1 mode mac EC:E5:55:D6:50:01`	To assign the static pool with index `1` to a client device with MAC address `EC:E5:55:D6:50:01`.
`dhcp-server pool modify 1 leasetime 172800`	To specify the lease time of the static pool with index `1`.
`dhcp-server pool mode 1 enable`	To enable the static pool with index `1`.
`dhcp-server operation`	To enable the DHCP server globally.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`dhcp-server operation`	To activate the DHCP server function on this port.

Setting up a dynamic pool

In the following example, you set up the device to assign an IP address from a certain address range to client devices connected to a certain port.

The dynamic pool is to be set up based on the following parameters:
- MAC address of the client device or further information in the DHCP request is not to be evaluated.
- Physical port to which the client devices are connected on the server device: `1/2`
- Address range from which the device assigns an IP address to the client devices: `192.168.23.92..192.168.23.142`
- The assigned IP settings are valid for 2 days: `172800`

Perform the following steps:

- ☐ Open the *Advanced > DHCP > DHCP Server > Pool* dialog.
- ☐ Add a table row. To do this, click the button.
- ☐ Specify the following settings for the table row:
  - *IP range start* column = `192.168.23.92`
  - *IP range end* column = `192.168.23.142`
  - *Port* column = `1/2`
  - *Lease time [s]* column = `172800`
  - *Active* column = `Marked`
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Advanced > DHCP > DHCP Server > Global* dialog.
- ☐ Verify that the DHCP function is active on port `1/2`.
  If not already done, mark the checkbox in the *DHCP server active* column for port `1/2`.
- ☐ Enable the DHCP server globally.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool add 2 dynamic 192.168.23.92 192.168.23.142`	To add a dynamic pool with index `2` with a range from `192.168.23.92` to `192.168.23.142`.
`dhcp-server pool modify 2 mode interface 1/2`	To assign the static pool with index `2` to physical port `1/2`.
`dhcp-server pool modify 2 leasetime 172800`	To specify the lease time of the dynamic pool with index `2`.
`dhcp-server pool mode 2 enable`	To enable the dynamic pool with index `2`.
`dhcp-server operation`	To enable the DHCP server globally.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`dhcp-server operation`	To activate the DHCP server function on this port.

15.1.3 Setting up a Preboot eXecution Environment (PXE)

The device lets you specify the boot parameters for PXE-compliant clients to boot a bootloader image downloaded from a TFTP server. Possible applications include booting an installation environment, a rescue system, or a live system over the network. A typical use case is an infotainment device that boots an operating system supplied over the network.

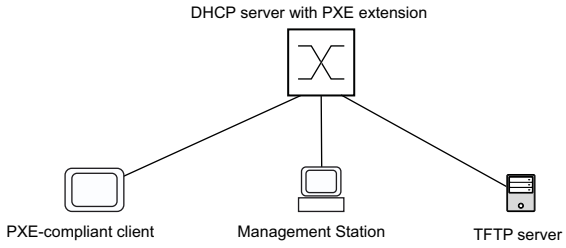


Figure 84: Simple structure of a Preboot eXecution Environment (PXE) setup

To activate the PXE boot extension for a specific pool, you add the following values to the pool settings:

- *Vendor Identifier*
- *Client System Architecture*
- URL to a bootloader image file on a TFTP server

The device expects the information for *Vendor Identifier* and *Client System Architecture* in summarized form as the *Class Identifier* in the DHCP option 60 field. When a PXE-compliant client device broadcasts a *DHCP Discover* message with a matching *Class Identifier* in the DHCP option 60 field, the device responds with the settings specified in the relevant pool.

A PXE-compliant client device requires a bootloader image that matches its hardware architecture. When planning, keep in mind that you need at least one pool for each required hardware architecture.

Note:
The device does not check the integrity, authenticity and availability of the TFTP servers and the bootloader image files involved. Use the PXE boot extension only if you trust the transfer network. Otherwise, undesirable behavior and security risks may result.

In the following example, the network administrator wants you to specify the PXE boot extension parameters for an existing *DHCP Server Pool* item.

Class Identifier in the DHCP option 60 field	*Vendor Identifier*	`vendor1`
	Client System Architecture	*`efi-x86-64`*
Bootloader image file on the TFTP server		`tftp://192.168.1.5/boot-efi-x86-64.img`

When modifying an existing *DHCP Server Pool* item, you need to deactivate the pool first. For information on how to set up a DHCP server pool, refer to section “Setting up a static pool” on page 368 or “Setting up a dynamic pool” on page 369. After modifying the *DHCP Server Pool* item, you reactivate the pool.

Perform the following steps:

- ☐ Open the *Advanced > DHCP > DHCP Server > Pool* dialog.
- ☐ Deactivate the *DHCP Server Pool* item. To do this, unmark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ In the *Vendor ID* column, enter the string `vendor1`.
- ☐ In the *Client Architecture* column, select the *efi-x86-64* item from the drop-down list.
- ☐ In the *Configuration URL* column, enter the URL: `tftp://192.168.1.5:/boot-efi-x86-64.img`.
- ☐ Reactivate the *DHCP Server Pool* item. To do this, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dhcp-server pool mode 1 disable`	To deactivate pool `1`.
`dhcp-server pool modify 1 mode classid vendorid vendor1`	To enable the PXE boot extension for pool `1` and assign the string `vendor1` as the *Vendor Identifier*.
`dhcp-server pool modify 1 mode classid architecture efi-x86-64`	To specify the value *efi-x86-64* as the *Client System Architecture*.
`dhcp-server pool modify 1 option configpath tftp://192.168.1.5:/boot-efi-x86-64.img`	To specify the URL `tftp://192.168.1.5/boot-efi-x86-64.img` to the bootloader image file on a TFTP server.
`dhcp-server pool mode 1 enable`	To reactivate pool `1`.
`show dhcp-server pool 1`	To display the settings specified for pool `1`.

```
DHCP Server Pool
----------------
Index.........................1
...
PXE Client Vendor ID............vendor1
PXE Client Architecture.........efi-x86-64
Configuration URL.............. tftp://192.168.1.5:/boot-efi-x86-64.img
...
```

15.2 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 the data packets 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.

15.2.1 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.

15.2.2 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*.

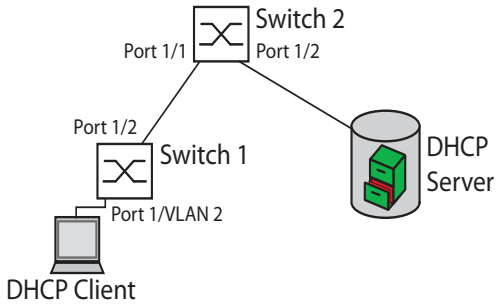


Figure 85: DHCP Layer 2 Example Network

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`.
- ☐ Enable the *DHCP L2 Relay* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply 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.
- ☐ Enable the *DHCP L2 Relay* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

Verify that VLAN 2 is present. Then perform the following steps on Switch 1:

- ☐ Set up VLAN 2, and add port 1/1 to VLAN 2.

`enable`	To change to the Privileged EXEC mode.
`vlan database`	To change to the VLAN configuration mode.
`dhcp-l2relay circuit-id 2`	To activate the Circuit ID and the DHCP Option 82 on VLAN 2.
`dhcp-l2relay remote-id ip 2`	To specify the IP address of the device as the Remote ID on VLAN 2.
`dhcp-l2relay mode 2`	To activate the *DHCP L2 Relay* function on VLAN 2.
`exit`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`dhcp-l2relay mode`	To activate the *DHCP L2 Relay* function on the port.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface 1/2.
`dhcp-l2relay trust`	To specify the port as *Trusted port*.
`dhcp-l2relay mode`	To activate the *DHCP L2 Relay* function on the port.
`exit`	To change to the Configuration mode.
`dhcp-l2relay mode`	To enable the *DHCP L2 Relay* function in the device.

Perform the following steps on Switch 2:

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface 1/1.
`dhcp-l2relay trust`	To specify the port as *Trusted port*.
`dhcp-l2relay mode`	To activate the *DHCP L2 Relay* function on the port.
`exit`	To change to the Configuration mode.
`interface 1/2`	To change to the Interface Configuration mode of interface 1/2.
`dhcp-l2relay trust`	To specify the port as *Trusted port*.

`dhcp-l2relay mode`	To activate the *DHCP L2 Relay* function on the port.
`exit`	To change to the Configuration mode.
`dhcp-l2relay mode`	To enable the *DHCP L2 Relay* function in the device.

15.3 Using the device as a DNS client

As a DNS client, the device queries a DNS server to resolve the hostname of a device in the network to the related IP address.

The device lets you specify up to 4 DNS servers to which it forwards a request to resolve a hostname (*DNS request*).

As an alternative, the device can obtain the DNS server addresses from a DHCP server. For this, the DHCP server needs to be reachable in the same VLAN as the management of the device.

The device lets you manually enter into the device the hostname and IP address of known devices in the network. You can enter up to 64 so-called static hosts.

When the device receives a request to resolve a hostname (*DNS request*), it first tries to find the related IP address internally. If the device cannot resolve the hostname by itself, it forwards the request to a DNS server. The DNS server returns the associated IP address to the device.

Optionally, the device caches this response for future queries. The device caches up to 128 DNS server responses consisting of hostname and related IP address.

15.3.1 Setting up the DNS client function

The device has the option to contact a DNS server assigned by the DHCP server. This example describes how to set up the device to contact a user-defined DNS server instead. To do this, perform the following steps:

- ☐ Open the *Advanced* > *DNS* > *Client* > *Static* dialog.
- ☐ In the *Configuration* frame, select the `user` item from the *Source* drop-down list.
- ☐ In the *Configuration* frame, *Domain name* field, specify the value `example.com`.
- ☐ In the table, click the button.
  The dialog displays the *Create* window.
- ☐ In the *Index* column, specify the value `1` as the sequential number. You can only assign unique values.
- ☐ In the *IP address* column, specify the IPv4 address of the DNS server, for example `192.168.3.5`. You can also specify a valid IPv6 address.
- ☐ Click the *Ok* button.
  The device adds a table row.
- ☐ Open the *Advanced* > *DNS* > *Client* > *Global* dialog.
- ☐ Enable the *Client* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dns client source user`	To specify that the device contacts a user-defined DNS server.

`dns client domain-name example.com`	To specify the string `example.com` as a domain name. The device adds this domain name to hostnames without a domain suffix.
`dns client servers add 1 ip 192.168.3.5`	To add a DNS server with the IPv4 address `192.168.3.5` as index `1`.
`dns client servers add 2 ip 2001::1`	To add a DNS server with the IPv6 address `2001::1` as index `2`.
`dns client adminstate`	To enable the *Client* function globally.

15.3.2 Setting up a static host

This example shows how to manually map an IP address to a hostname. To do this, perform the following steps:

- ☐ Open the *Advanced* > *DNS* > *Client* > *Static Hosts* dialog.
- ☐ In the table, click the button.
  The dialog displays the *Create* window.
- ☐ In the *Index* column, specify the value `1`.
- ☐ In the *Hostname* column, enter the hostname, for example `device1`.
- ☐ In the *IP address* column, specify the IPv4 address to be mapped to the hostname, for example `192.168.3.9`. You can also specify a valid IPv6 address.
- ☐ Click the *Ok* button.
  The device adds a table row. The device sends data packets directed to `device1` to the recipient with the IP address `192.168.3.9`.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`dns client host add 1 name device1 ip 192.168.3.9`	To map the hostname `device1` with the IP address `192.168.3.9`.
`dns client adminstate`	To enable the *Client* function globally.

15.4 GARP function

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE standards association 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.

15.4.1 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.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`garp gmrp operation`	To enable the *GMRP* function on the port.
`exit`	To change to the Configuration mode.
`garp gmrp operation`	To enable the *GMRP* function globally.

15.4.2 Configuring GVRP

You use the *GVRP* function to allow the device to exchange VLAN configuration information with other *GVRP*-capable devices. Thus reducing unnecessary traffic of Broadcast and unknown Unicast data packets. Besides, the *GVRP* function dynamically sets up 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*-capable devices. To do this, perform the following steps:

- ☐ Open the *Switching* > *GARP* > *GVRP* dialog.
- ☐ To exchange VLAN configuration information with other *GVRP*-capable devices, mark checkbox in the *GVRP active* column for the port.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 3/1`	To change to the Interface Configuration mode of interface `3/1`.
`garp gvrp operation`	To enable the *GVRP* function on the port.
`exit`	To change to the Configuration mode.
`garp gvrp operation`	To enable the *GVRP* function globally.

15.5 MRP-IEEE

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP-IEEE) to replace the Generic Attribute Registration Protocol (GARP). The IEEE standards association 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 forwarding the data packets to the required areas of a network, the MRP-IEEE applications distribute attribute values to MRP-IEEE enabled devices across a LAN. The MRP-IEEE applications register and de-register Multicast group memberships and VLAN identifiers.

Note:
The Multiple Registration Protocol (MRP-IEEE) requires a loop free network. To help prevent loops in the network, use a network protocol such as the Media Redundancy Protocol (MRP), Spanning Tree Protocol (STP), or Rapid Spanning Tree Protocol (RSTP) with MRP-IEEE.

15.5.1 MRP-IEEE 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-IEEE 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-IEEE 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 data packets.

15.5.2 MRP-IEEE timers

The default timer settings help prevent unnecessary attribute declarations and withdrawals. The timer settings allow the participants to receive and process MRP-IEEE 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, even if there is a lost message, specify the *Leave* timer value ≥ (2x JoinTime) + 60 in 1/100 s.
- To minimize the volume of *Rejoin* data packets the device generates following a *LeaveAll* event, specify the value for the *LeaveAll* timer larger than the *Leave* timer value.

The following list contains various MRP-IEEE 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 withdrawal state.
- *LeaveAll*
  Controls the frequency with which the switch generates *LeaveAll* messages.

When expired, the Periodic timer initiates a Join request MRP-IEEE message that the switch sends to participants on the LAN. The switches use this message to help prevent unnecessary withdrawals.

15.5.3 MMRP

When a device receives Broadcast, Multicast or unknown data packets on a port, the device floods the data packets to the other ports. This process causes unnecessary use of bandwidth on the LAN.

The Multiple MAC Registration Protocol (MMRP) lets you control the data packets 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-IEEE 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.

To maintain the registration and deregistration state and to receive data packets, a port declares interest periodically. Every device on a LAN with the *MMRP* function enabled maintains a filtering database and forwards the data packets with the group MAC addresses to the listed participants.

Setting up MMRP

In this example, Host A intends to listen to the data packets destined for 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 the data packets 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.

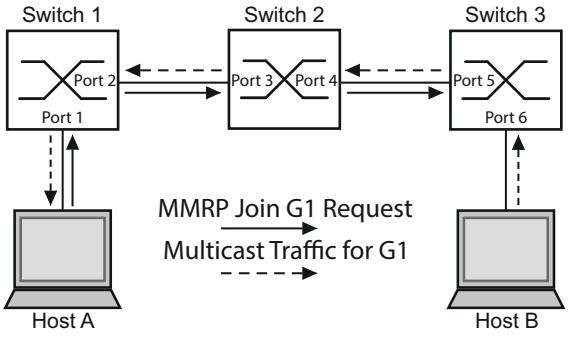


Figure 86: MMRP Network for MAC address Registration

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.
- ☐ Apply 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`mrp-ieee mmrp operation`	To enable the *MMRP* function on the port.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`mrp-ieee mmrp operation`	To enable the *MMRP* function on the port.
`exit`	To change to the Configuration mode.
`mrp-ieee mrp periodic-state-machine`	To enable the *Periodic state machine* function globally.
`mrp-ieee mmrp operation`	To enable the *MMRP* function globally.

15.5.4 MVRP

The Multiple VLAN Registration Protocol (MVRP) is an MRP-IEEE application that provides dynamic VLAN registration and withdrawal 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 the data packets 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.

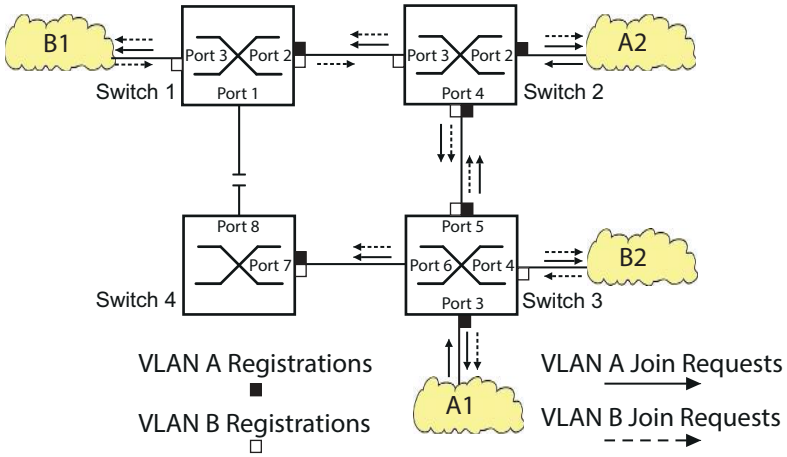


Figure 87: MVRP Example Network for VLAN Registration

In the MVRP example network, the LANs first send a Join request to the switches. The switch enters the VLAN registration in the MAC address table (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 MAC address table (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.
- ☐ Enable the *MVRP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`mrp-ieee mvrp operation`	To enable the *MVRP* function on the port.
`interface 1/2`	To change to the Interface Configuration mode of interface `1/2`.
`mrp-ieee mvrp operation`	To enable the *MVRP* function on the port.
`exit`	To change to the Configuration mode.
`mrp-ieee mvrp periodic-state-machine`	To enable the *Periodic state machine* function globally.
`mrp-ieee mvrp operation`	To enable the *MVRP* function globally.

16 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 first active optical LAN 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.

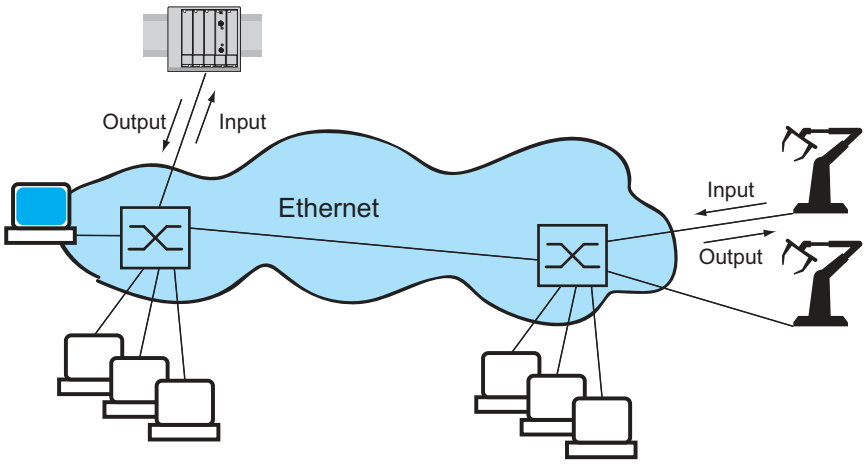


Figure 88: Example of communication.

16.1 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.

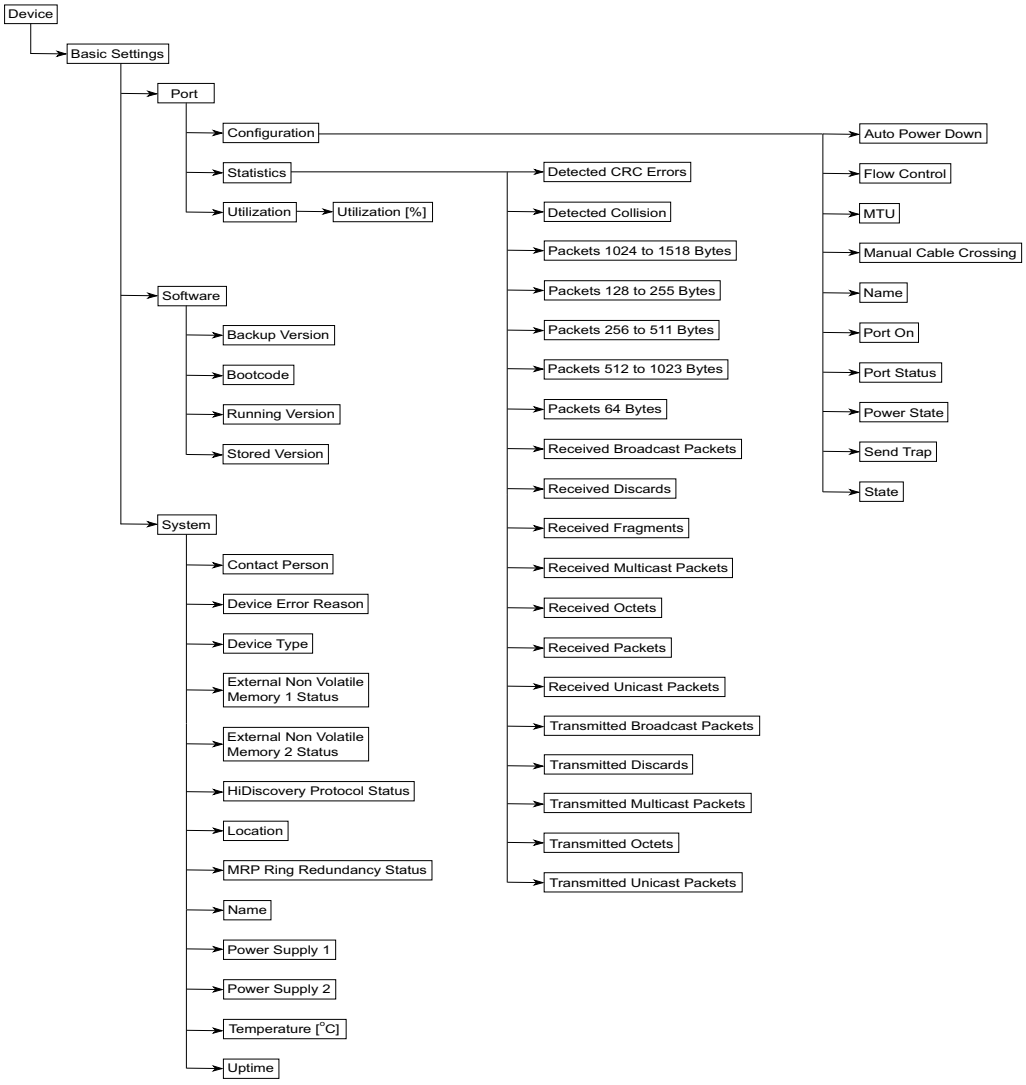


Figure 89: OPC UA information model

Table 47: Objects in the OPC UA information model

Object	Description
Power save	Specifies how the port behaves when no cable is connected.
Port on	Activates/deactivates the port.
Power state	Specifies if the port is physically switched on or off when you deactivate the port with the *Port on* function.
State	Displays if the port is currently physically enabled or disabled.
Port status	Displays the link status of the port.

Table 48: Object values in the OPC UA information model

Object	Value	Description
Device Error Reason	1	None
	2	Power supply
	3	Link failure
	4	Temperature
	5	Fan failure
	6	Module removal
	7	External non volatile memory removal
	8	External non volatile memory not in synchronization
	9	Ring redundancy
External Non Volatile Memory 1 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
External Non Volatile Memory 2 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
HiDiscovery Protocol Status	1	Enabled
	2	Disabled
MRP Ring Redundancy Status	1	Available
	2	Not available
Power Supply 1	1	Present
	2	Defective
	3	Not installed
	4	Unknown
Power Supply 2	1	Present
	2	Defective
	3	Not installed
	4	Unknown

Table 48: Object values in the OPC UA information model

Object	Value	Description
Auto Power Down	1	Auto power down
	2	No power save
	3	Energy efficient ethernet
	4	Unsupported
Flow Control	1	Enabled
	2	Disabled
Manual Cable Crossing	1	Medium dependent interface
	2	Medium dependent interface crossover
	3	Auto medium dependent interface crossover
	4	Unsupported
Port On	1	Up
	2	Down
	3	Testing
Power State	1	Enabled
	2	Disabled
Send Trap	1	Enabled
	2	Disabled
State	1	Up
	2	Down
Port Status	1	Up
	2	Down
	3	Testing
	4	Unknown
	5	Dormant
	6	Not present
	7	Lower layer down

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.

16.1.1 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.
- ☐ Enable the *OPC UA Server* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply 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.
- ☐ Apply 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`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`opc-ua operation`	To enable the *OPC UA Server* server.
`opc-ua port <1..65535>`	To change the TCP port number, if necessary.
`opc-ua sessions <1..5>`	To specify the number of *OPC UA* connections that can be established simultaneously.
`opc-ua security-policy none | basic128rsa15 | basic256 | basic256sha256`	To specify the authentication and encryption protocol.
`show opc-ua global`	To display the *OPC UA* Server settings.

```
IEC62541 - OPC/UA server settings
-------------------------
IEC62541 - OPC/UA server operation.........enabled
Listening port.............................4840
Number of concurrent sessions..............5
Configured security-policy.................none
```

16.1.2 Setting up an OPC UA user account

The device lets you manage the *OPC UA* user accounts required to access the device using a *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, you 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:

- ☐ Open the *Advanced > Industrial Protocols > OPC UA Server* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
- ☐ Enter the name `USER` in the *User name* field.
- ☐ Click the *Ok* button.
- ☐ In the *Password* field, enter a password of at least 6 characters.
  In this example, you give the user account the password `SECRET`.
- ☐ In the *Access role* column, select the *readOnly* item.
- ☐ Apply 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.
  The dialog displays the *OPC UA* user accounts that are set up.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`users add USER`	To add the *OPC UA* user account `USER`.

`opc-ua users modify USER password`
`Enter NEW password: ****** (SECRET)`
`Confirm NEW password: ****** (SECRET)`
	To enter and confirm the password `SECRET` for the *OPC UA* user account `USER`. Enter a password of at least 6 characters.

`opc-ua users modify USER access-role read-only`	To assign the access role *readOnly* to the *OPC UA* user account `USER`.
`opc-ua users enable USER`	To activate the user account `USER`.
`show opc-ua users`	To display the user accounts that are set up.

```
User Name                 Access-Role      Status
------------------------- ---------------- ------
user                      read-only        [x]
```

Note:
When you set up a new *OPC UA* user account, remember to set the password.

16.1.3 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.
- ☐ Apply 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                                  To change to the Privileged EXEC mode.
configure                               To change to the Configuration mode.
opc-ua users disable USER               To disable the user account USER.
show opc-ua users                       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.
```

16.1.4 Deleting 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.
- ☐ Apply 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                                  To change to the Privileged EXEC mode.
configure                               To change to the Configuration mode.
opc-ua users delete USER                To delete the user account USER.
```

```
show opc-ua users
User Name                 Access-Role   Status
------------------------- ------------- ------

save
```

To display the user accounts that are set up.

To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

16.2 Service Discovery

Service Discovery is part of a series of technologies summarized by the term Zero-configuration networking (zeroconf). Service Discovery uses multicast DNS (mDNS) and DNS service discovery (DNS-SD) to advertise the services offered by the device to other devices in the network that request the service. The device currently supports the *ITxPT Module Inventory* service. Additional services may follow in future releases.

Devices that support Service Discovery can automatically discover the available services on the network without having information about which devices are available. In public transportation, for example, such devices can be ticketing systems, passenger information systems, or vehicle tracking systems.

Devices that subscribe to the services will detect a new device as soon as you connect it to the network, and read its service data. For example, when you install a ticketing system in the network of a public transportation vehicle, the ticketing system needs to communicate with the existing passenger information system to deliver real-time updates on ticket sales and availability.

16.2.1 ITxPT Module Inventory

The *ITxPT Module Inventory* service is part of the Information Technology for Public Transport (ITxPT) specification.

The intended use of the *ITxPT Module Inventory* service is module inventory in networks of vehicles. The *ITxPT Module Inventory* service lets devices subscribing to the service automatically inventory the modules installed in the on-board IP network of vehicles. Modules in the sense of ITxPT might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. The service lets you collect information about the modules and monitor their status.

The device provides the information through *SRV records* and *TXT records*.

- The *SRV record* contains the location.
- The device provides the *TXT record* through mDNS. The *TXT record* contains information about the service.
  - `version`
    Version of the related ITxPT specification release
    Example: `2.1.2`
  - `type`
    Short name of the device type
    Example: `MESW (Managed Ethernet Switch)`
  - `model`
    Name of the device
    For example, the product code
    Example: `DRAGON-00484`
  - `manufacturer`
    Manufacturer of the device
    Example: `Hirschmann Automation and Control GmbH`
  - `serialnumber`
    Serial number of the device
    Example: `942287999020501939`
  - `softwareversion`
    Software version installed on the device
    Example: `DRAGON-00484 Release HiOS-2A-10.6.002026-10-03 09:34`

- `hardwareversion`
  Hardware version of the device
  Example: `0202`
- `macaddress`
  MAC address of the device in hexadecimal format
  Example: `CF:DA:98:63:9D:F6`
- `status`
  Integer containing the last detected error
  The value `0` means: No error detected.
  Example: `C0FFFFFFFFF3FFFF01FCFFFF FFFFFFFF`
- `xstatus`
  Detailed device status
  For example, the status of the ports participating in the *ITxPT Module Inventory* service
  Example: `C0FFFFFFFFF3FFFF01FCFFFF FFFFFFFF`
- `services`
  List of available services on the device
  For example, the *ITxPT Module Inventory* service
  Example: `inventory`

The device transmits the *TXT record* once in the following cases:

- After an mDNS query containing the address `_itxpt_socket._tcp.local`
  The device transmits the *TXT record* in response to multicast or unicast requests in the network for services offered by the device.
- Without a request
  - As soon as the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled. See the *Operation* frame.
  - If the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled, and the device detects changes regarding the global status or the port status of other devices in the network. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

16.2.2 Application example

The following example illustrates a typical use case in the field of public transportation. The vehicle on-board network contains, in addition to switches and the management station, the on-board passenger information system, the on-board remote diagnostic system, and other devices typical for this application.

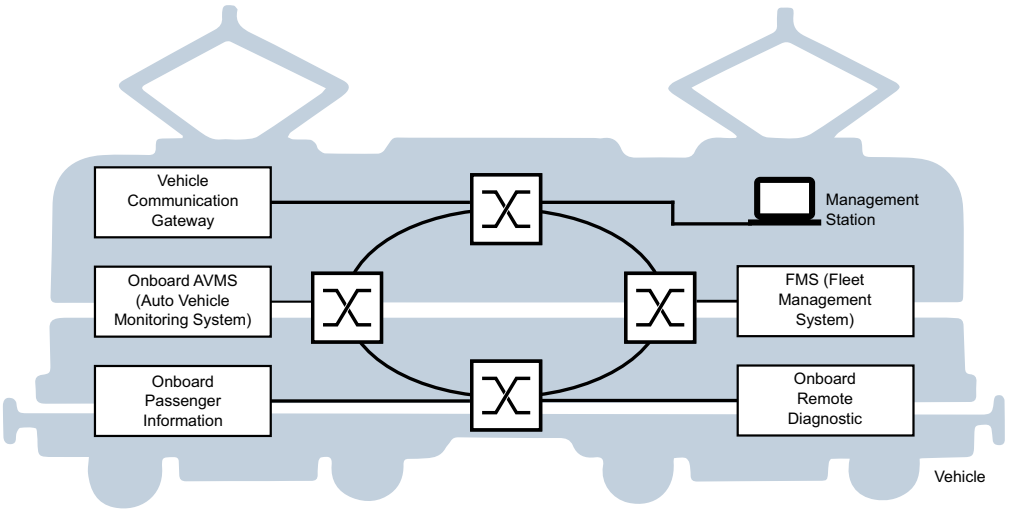


Figure 90: Example for ITxPT Module Inventory

Enabling the Service Discovery function on the device

Enable the *Service Discovery* function on every switch in the on-board network. Simultaneously, the device activates the *ITxPT Module Inventory* service to monitor the link status or the PoE status of the device.

Perform the following steps:

- ☐ Enable the *Service Discovery* function and activate the *ITxPT Module Inventory* service on the device.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`service-discovery operation`	To enable the *Service Discovery* function and to activate the *ITxPT Module Inventory* service.
`show service-discovery global`	To display the *Service Discovery* and the *ITxPT Module Inventory* settings of the device.

Enabling the link status monitoring per port

For each required port, activate the *ITxPT Module Inventory* service to monitor the link status of the port.

Perform the following steps:

- ☐ In the table, in the *Link* column, mark the checkbox for the port.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`service-discovery monitor link`	To activate the *ITxPT Module Inventory* service to monitor the link status of the port.
`show service-discovery port`	To display the *Service Discovery* and the *ITxPT Module Inventory* settings per port.
`exit`	To change to the Configuration mode.

Enabling the PoE status monitoring per port

For each required port, activate the *ITxPT Module Inventory* service to monitor the PoE status of the port.

Perform the following steps:

- ☐ In the table, in the *PoE* column, mark the checkbox for the port.
- ☐ Apply the settings temporarily. To do this, click the  button.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`service-discovery monitor poe`	To activate the *ITxPT Module Inventory* service to monitor the PoE status of the port.
`show service-discovery port`	To display the *Service Discovery* and the *ITxPT Module Inventory* settings per port.
`exit`	To change to the Configuration mode.

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.

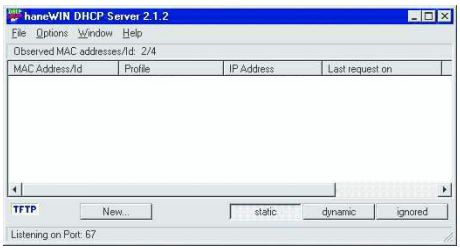


Figure 91: Start window of the haneWIN DHCP Server program

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.



Figure 92:DHCP setting

- ☐ Click the *OK* button.
- ☐ To enter the configuration profiles, click in the menu bar the items *Options > Configuration Profiles*.

☐ Specify the name for the new configuration profile.

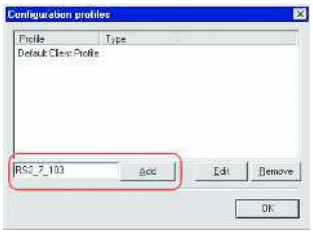


Figure 93:Adding configuration profiles

☐ Click the *Add* button.
☐ Specify the netmask.

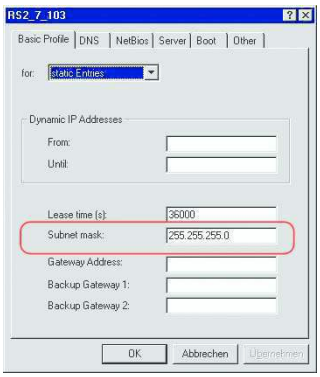


Figure 94:Netmask in the configuration profile

☐ 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.

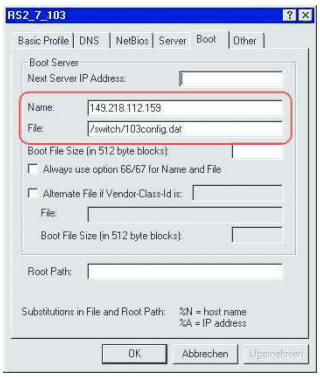


Figure 95:Configuration file on the tftp server

☐ 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.

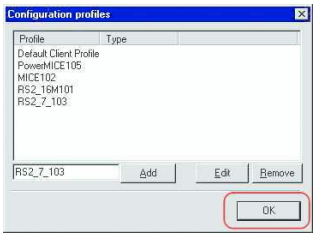


Figure 96:Managing configuration profiles

☐ 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.

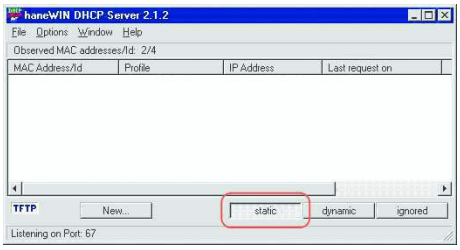


Figure 97:Static address input

☐ Click the *Add* button.

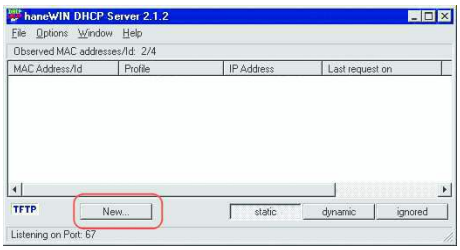


Figure 98:Adding static addresses

☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.

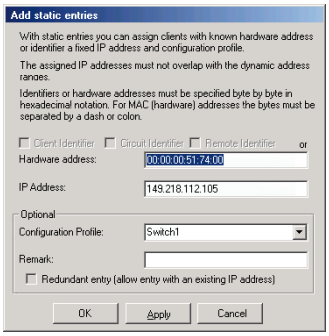


Figure 99:Entries for static addresses

☐ 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.

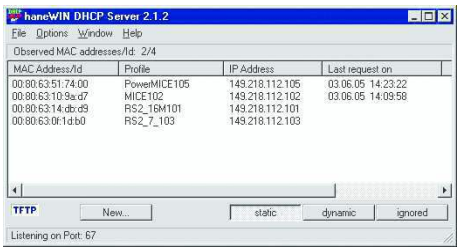


Figure 100:DHCP server with entries

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.

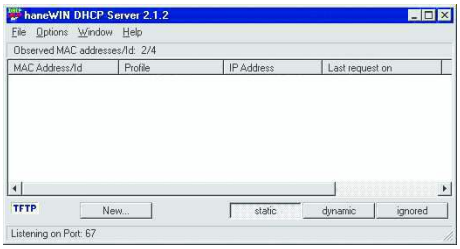


Figure 101: Start window of the haneWIN DHCP Server program

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.

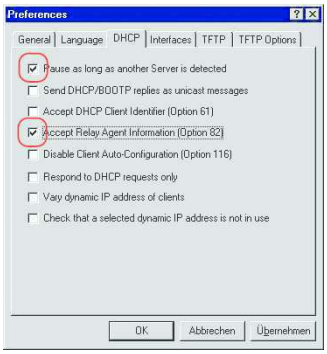


Figure 102: DHCP setting

- ☐ To enter the static addresses, click the *Add* button.

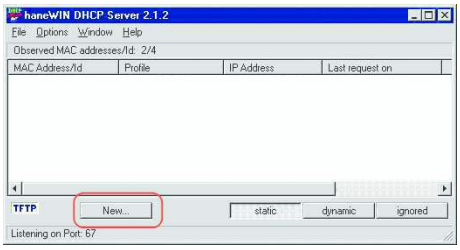


Figure 103: Adding static addresses

- ☐ Mark the *Circuit Identifier* checkbox.
- ☐ Mark the *Remote Identifier* checkbox.

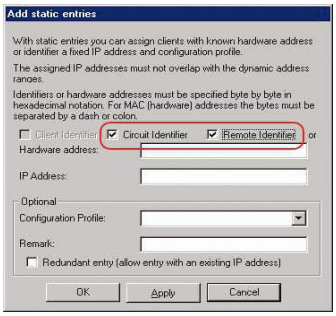


Figure 104: Default setting for the fixed address assignment

- ☐ 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:
  `ciclhhvvvvssmmpprirlxxxxxxxxxxxx`
  - `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
  - `ss`
    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.
  - `ri`
    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 105: Specifying the addresses

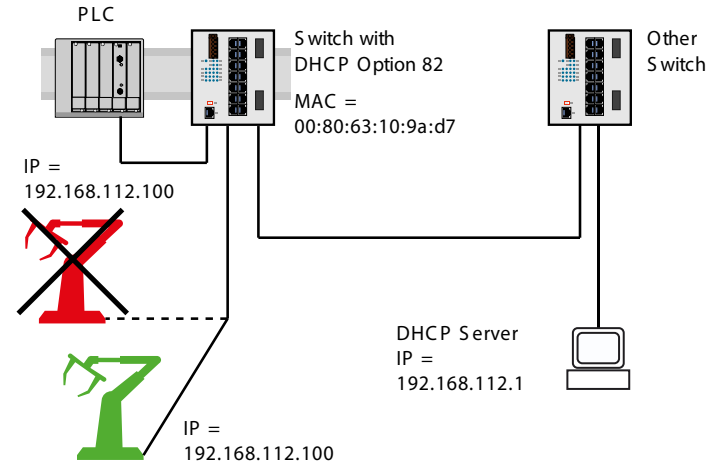


Figure 106: Application example of using Option 82

A.3 HTTPS certificate

Your web browser establishes the connection to the device using the Hypertext Transfer Protocol Secure (HTTPS). The prerequisite is that you enable the *HTTPS server* function in the*Device Security > Management Access > Server* dialog, *HTTPS* tab.

A.3.1 Conflicts in certificate validation

Web browsers and other third-party software routinely validate digital certificates.

If your web browser displays a message indicating a conflict in validating the digital certificate of the device, perform the following steps:

- ☐ Verify if the digital certificate has expired.
- ☐ Verify if your web browser no longer regards the algorithm used for generating the digital certificate as trustworthy.

To solve the conflict in certificate validation, update the digital certificate on the device. See section “HTTPS certificate management”.

A.3.2 HTTPS certificate management

To establish a secure connection, a digital certificate in X.509 format is required. In the default setting, the device uses a self-signed digital certificate.

You can regenerate the self-signed digital certificate using the latest device software. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ To generate a self-signed digital certificate, in the *Certificate* frame, click the *Create* button.
- ☐ Apply the settings temporarily. To do this, click the  button.
- ☐ For the changes to take effect after transferring a digital certificate onto the device, disable and re-enable the HTTPS server. Restart the HTTPS server using the Command Line Interface.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https certificate generate`	To generate a digital certificate for the HTTPS server.
`no https server`	To disable the *HTTPS* function.
`https server`	To enable the *HTTPS* function.

As an alternative, generate a digital certificate externally, using up-to-date signature algorithms. Transfer the new digital certificate onto the device. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTPS* tab.
- ☐ When the file is located on your PC or on a network drive, drag and drop it onto the area. As an alternative, click in the area to select the file.
- ☐ To transfer the file to the device, click the *Start* button.
- ☐ Apply the settings temporarily. To do this, click the button.

`enable`	To change to the Privileged EXEC mode.
`copy httpscert envm <file name>`	To transfer the digital certificate for the HTTPS server from the external memory (*ENVM*) onto the device.
`configure`	To change to the Configuration mode.
`no https server`	To disable the *HTTPS* function.
`https server`	To enable the *HTTPS* function.

Note:
To activate the digital certificate after the device generated or you transferred it, reboot the device or restart the HTTPS server. Restart the HTTPS server using the Command Line Interface.

A.3.3 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.
- ☐ Enable the *HTTPS* 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.

`enable`	To change to the Privileged EXEC mode.
`configure`	To change to the Configuration mode.
`https port 443`	To specify the number of the TCP port on which the web server receives HTTPS requests from clients.
`https server`	To enable the *HTTPS* function.
`show https`	To display the status of the *HTTPS* server and the port number.

When you make changes to the HTTPS port number, disable the HTTPS server and enable it again to make the changes effective.

The device uses Hypertext Transfer Protocol Secure (HTTPS) and establishes a new data connection. When you log out at the end of the session, the device terminates the data connection.

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, Axel Schneider
  Wiley, 2018
  ISBN 978-1-119-52791-6 (Print), ISBN 978-1-119-52799-2 (eBook)
- *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
  ISBN 978-1-449-31921-2 (Print)
- *TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition)* (in English)
  W. R. Stevens, Kevin R. Fall
  Addison Wesley, 2011
  ISBN 978-0-321-33631-6
- *Measurement, Control and Communication Using IEEE 1588* (in English)
  John C. Eidson
  Springer, 2006
  ISBN 978-1-84628-250-8 (Print), ISBN 978-1-84628-251-5 (eBook)
- *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 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.

Definition of the syntax terms used:	
Integer	An integer in the range $-2^{31}..2^{31}-1$
IP address	`xxx.xxx.xxx.xxx` (`xxx` = integer in the range `0..255`)
MAC address	12-digit hexadecimal number in accordance with ISO/IEC 8802-3
Object Identifier	x.x.x.x… (for example 1.3.6.1.1.4.1.248...)
Octet String	ASCII character string
PSID	Power supply identifier (number of the power supply unit)
TimeTicks	Stopwatch, Elapsed time = numerical value / 100 (in seconds) numerical value = integer in the range $0..2^{32}-1$
Timeout	Time value in hundredths of a second time value = integer in the range $0..2^{32}-1$
Type field	4-digit hexadecimal number in accordance with ISO/IEC 8802-3
Counter	Integer ($0..2^{32}-1$), when certain events occur, the value increases by `1`.

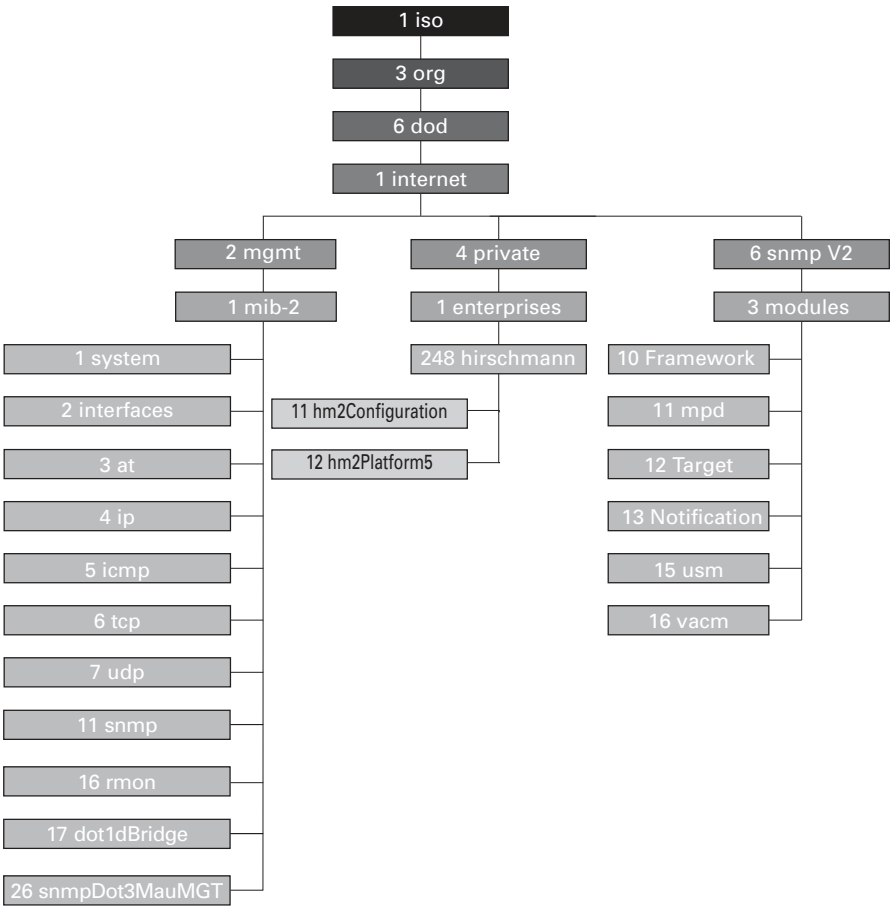


Figure 107: Tree structure of the Hirschmann MIB

When you have downloaded updated device software from the product pages on the Internet, the ZIP archive contains not only the device software but also the MIBs.

B.3 List of RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB

RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD syslog protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6

RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.4 Underlying IEEE Standards

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.5 Underlying IEC Norms

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.6 Underlying ANSI Norms

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.7 Technical Data

B.7.1 Switching

Size of the MAC address table (forwarding database) (incl. static filters)	32768
Max. number of statically set-up MAC address filters	100
Max. number of MAC address filters learnable through IGMP Snooping	1024
Max. number of MAC address entries (MMRP)	512
Number of priority queues	8 Queues
Port priorities that can be set	0..7
MTU (Max. allowed length of packets a port can receive or transmit)	12288 Bytes

B.7.2 VLAN

VLAN ID range	1..4042
Number of VLANs	max. 512 simultaneously per device max. 512 simultaneously per port

B.7.3 Access Control Lists (ACL)

Max. number of ACLs	100
Max. number of rules per ACL	1023
Max. number of rules per port	1023
Number of total configurable rules	16368 (16 × 1023)
Max. number of VLAN assignments	48
Max. number of rules which log an event	128
Max. number of Ingress rules	3584 (7168)
Max. number of Egress rules	1024 (2048)

B.8 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.9 Abbreviations used

ACA	Name of the external memory
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted-pair

UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

0-9
2-Switch coupling, Primary device . . . 278
2-Switch coupling, Stand-by device . . . 280
802.1X . . . 66

A
Access roles . . . 69
Access security . . . 129
Advanced Information, HIPER Ring . . . 227
Advanced Information, MRP . . . 217
Advanced Information, RCP . . . 289
Advanced Information, Ring/Network Coupling . . . 269
Advanced Information, Sub Ring . . . 256
Advanced mode . . . 216, 219
AF . . . 188
Aging time . . . 171
Alarm . . . 304
Alarm messages . . . 303
Alternate port . . . 238, 244
APNIC . . . 44
ARIN . . . 44
ARP . . . 46
Assured Forwarding . . . 188
Authentication list . . . 66
Automatic configuration . . . 130

B
Backup port . . . 239, 244
Bandwidth . . . 191
Best Master Clock algorithm . . . 102
BOOTP . . . 43
Boundary clock (PTP) . . . 101
BPDU . . . 233
BPDU guard . . . 243, 244
Bridge Identifier . . . 230
Bridge Protocol Data Unit . . . 233

C
CA (Certification Authority) . . . 77, 338
Certificate . . . 338
Certification Authority (CA) . . . 77, 338
CIDR . . . 46
Class Selector . . . 188
Classless inter domain routing . . . 46
Closed circuit . . . 313
Command Line Interface . . . 19
Command tree . . . 27
Configuration file . . . 60
Configuration modifications . . . 303

D
Data stream monitoring Port Mirroring . . . 341
Data stream monitoring VLAN Mirroring . . . 343
Data stream monitoring, RSPAN . . . 345
Data traffic . . . 151
Delay (PTP) . . . 102
Delay measurement (PTP) . . . 102
Delay time (MRP) . . . 216
Denial of Service . . . 151
Designated bridge . . . 238
Designated port . . . 238, 243
Destination table . . . 303
Device replacement . . . 15
Device status . . . 305
DHCP . . . 43
DHCP L2 Relay . . . 372
DHCP server . . . 94, 98, 367, 397, 400
DHCPv6 . . . 61
Diameter (Spanning Tree) . . . 232
Differentiated services . . . 188
DiffServ . . . 177
DiffServ Codepoint . . . 188
Digital certificate . . . 338
Disabled port . . . 239
DoS . . . 151
DSCP . . . 177, 186, 188

E
Edge port . . . 238, 243
EF . . . 188
Email notification . . . 328
Event log . . . 336
Expedited Forwarding . . . 188

F
FDB (MAC address table) . . . 167
First installation . . . 43
Flow control . . . 191

G
GARP . . . 378
Gateway . . . 44, 53
Generic object classes . . . 408
Global Config mode . . . 25
GMRP . . . 378
Grandmaster (PTP) . . . 102

H
HaneWin . . . 397, 400
Hardware reset . . . 303
HiDiscovery . . . 43
HIPER Ring . . . 226
HIPER Ring Advanced Information . . . 227
HIPER Ring Packet Prioritization . . . 228
HIPER Ring Packets . . . 227
HiView . . . 65
Host address . . . 44

I

IANA . . . 44
IAS . . . 66
IEEE MAC address . . . 322
IEEE 802.1X . . . 66
IGMP snooping . . . 171
Industrial HiVision . . . 13
Instantiation . . . 408
Integrated Authentication Server . . . 66
Interface status . . . 295
Interface tracking . . . 295, 298
Interface tracking object . . . 295
IP address . . . 44, 53, 60
IP header . . . 177, 179, 188
IPv6 address . . . 48
IPv6 address types . . . 49
ISO/OSI layer model . . . 46

L

LACNIC . . . 44
LDAP . . . 66
Leave message . . . 171
Link Aggregation . . . 213
Link Aggregation interface . . . 295
Link down delay . . . 296
Link monitoring . . . 305, 313
Link up delay . . . 296
Logical tracking . . . 295, 297
Login dialog . . . 18
Loop guard . . . 244, 246
Loops . . . 279, 280, 283, 285

M

MAC address filter . . . 167
MAC destination address . . . 46
MAC address table (forwarding database) . . . 167
MaxAge . . . 233
Memory (RAM) . . . 105
Message . . . 303
Mode . . . 130
MRP . . . 212, 213, 215, 216
MRP Advanced Information . . . 217
MRP over LAG . . . 222
MRP Packet Prioritization . . . 218
MRP Packets . . . 217
MRP-IEEE . . . 380
MRP-IEEE operation . . . 380
MRP-IEEE timers . . . 380
Multicast . . . 171

N

Netmask . . . 44, 53
Network load . . . 229, 230
Network management . . . 61
Network structure . . . 215, 222
Non-volatile memory (NVM) . . . 105
NVM (non-volatile memory) . . . 105

O

Object classes 408
Object description 408
Object ID 408
OpenSSH 21, 145
Operation monitoring 313
Operators 297
Option 82 400
Ordinary clock (PTP) 102

P

Path costs 231, 234
PHB 188
Polling 303
Port Identifier 230
Port Mirroring 341
Port priority 185
Port roles (RSTP) 238
Port State 239
Precedence 188
Prefix length 49
Primary ring (RCP) 287
Priority 179
Priority queue 180
Priority tagged frames 179
Privileged Exec mode 24
Protection functions (guards) 243
PTP 93
PTP domain 103
PuTTY 19, 21, 39

Q

QoS 178
Query 171

R

RADIUS . . . 66
RAM (memory) . . . 105
Rapid Spanning Tree . . . 212, 213, 238
RCP . . . 213
RCP Advanced Information . . . 289
RCP packets . . . 290
RCP prerequisites . . . 289
RCP topology requirements . . . 290
RCP, Topology of Two-Switch Redundant Coupling . . . 289
RCP, Topology Overview . . . 289
Real time . . . 177
Reconfiguration . . . 230
Reconfiguration time (MRP) . . . 216
Redundancy . . . 229
Reference time source . . . 93, 98, 102
Relay contact . . . 313
Remote diagnostics . . . 313
Remote Switch Port Analyzer . . . 345
Report . . . 333
Report message . . . 171
RFC . . . 410
Ring . . . 215, 222
Ring Manager . . . 215, 222
Ring/Network coupling . . . 213
Ring/Network Coupling Advanced Information . . . 269
Ring/Network Coupling packet prioritization . . . 274
Ring/Network Coupling packets . . . 272
Ring/Network coupling, Link Topology of 1-Switch coupling . . . 269
Ring/Network coupling, Link Topology of 2-Switch coupling . . . 270
Ring/Network coupling, Link Topology of 2-Switch coupling with Control Line . . . 271
Ring/Network Coupling, Topology requirements . . . 274
RIPE NCC . . . 44
RM (Ring Manager) . . . 215, 222
RMON probe . . . 341
Root bridge . . . 234
Root guard . . . 243, 246
Root path . . . 235, 236
Root path cost . . . 230
Root port . . . 238, 244
Router . . . 44
Router Advertisement Daemon . . . 58, 62
RSPAN . . . 345
RSPAN combined source/intermediate role . . . 350
RSPAN destination role . . . 349
RSPAN device roles . . . 349
RSPAN example with reflector port . . . 354
RSPAN example without reflector port . . . 358
RSPAN example, starting point . . . 354
RSPAN interaction with Link Aggregation . . . 353
RSPAN interaction with Spanning Tree . . . 353
RSPAN intermediate role . . . 350
RSPAN line topology . . . 346
RSPAN over ring redundancy protocols . . . 352
RSPAN packet prioritization . . . 353
RSPAN purpose . . . 345
RSPAN Reflector port properties . . . 351
RSPAN ring topology . . . 347
RSPAN source role . . . 349

RSPAN topologies 345
RSPAN tree topology 346
RSPAN uplink properties 351
RSPAN VLAN properties 348
RSPAN with redundancy 352
RST BPDU 238, 240
RSTP 241

S

Secondary ring (RCP) 287
Secure Shell (SSH) 21
Segmentation 303
Serial connection 19, 39
Service 333
Service Shell 24
Service Shell deactivation 37
Setting the time 93
SFP module 321
Signal contact 313
SNMP 303
SNMP trap 303, 304
SNTP 93
Software version 119
SSH (Secure Shell) 21
Static routing 295
Store-and-forward 167
STP-BPDU 233
Strict Priority 180
Sub Ring 213, 254
Sub Ring Advanced Information 256
Sub Ring Manager 265
Sub Ring Packet Prioritization 257
Sub Ring Packets 256
Sub Ring Redundant Manager 265
Subidentifier 408
Subnet 53
Syslog over TLS 338
System Monitor 1 39
System requirements (Graphical User Interface) 17
System time 93

T

Tab Completion 34
TACACS+ 66
TACACS+ accounting 91
TCN guard 244, 246
Technical Documents 429
Technical questions 429
Technical Support 429
Topology Change flag 244
ToS 177, 179, 188
Tracking (VRRP) 295
Traffic class 180, 185
Traffic shaping 186
Training courses 429
Transmission reliability 303
Transparent clock (PTP) 101
Trap 303, 304
Trap destination table 303
Tree structure (Spanning Tree) 234, 237
Type of Service 179

U

User Exec mode 24
User name 18, 20, 22
Utilization 229, 230

V

Video 180
VLAN 193
VLAN (HIPER Ring) 226
VLAN Mirroring 343
VLAN mode 24
VLAN priority 184
VLAN router interface 295
VLAN tag 179, 193
VoIP 180
VRRP Tracking 295
VT100 terminal emulation 19, 39

W

Weighted Fair Queuing 180
Weighted Round Robin 180

D Technical 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.belden.com.

For technical support, visit my.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/services/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:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

User Manual

Security
DRAGON Switch
HiOS-2A

Technical support
https://hirschmann-support.belden.com

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.

© 2026 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

Safety instructions . . . 9

Safety information . . . 10

About this Manual . . . 11

Key . . . 12

Synopsis . . . 13
Audience . . . 13

1 Security planning . . . 15
1.1 Basics . . . 15
1.1.1 Security terminology . . . 15
1.1.2 Convenience vs. security: Navigating the field of tension . . . 17
1.1.3 Skepticism vs. optimism: qualitative security philosophy . . . 18
1.1.4 Impartial assessment . . . 18
1.1.5 Threat analysis . . . 19
1.1.6 Mitigation: confidentiality example . . . 19
1.1.7 Theoretical and practical degrees of security . . . 20
1.1.8 Strategies to provide improved security: confidentiality example . . . 20
1.1.9 Skepticism: Approximations in this document . . . 20
1.2 Overview . . . 21
1.2.1 Subject . . . 21
1.2.2 Scope . . . 21
1.2.3 Capability security levels . . . 22
1.2.4 Required preparatory work . . . 22
1.2.5 Software setup scenarios and hardware scenarios . . . 24
1.2.6 Scenario development . . . 25
1.3 Compiling a threat profile . . . 26
1.3.1 Risk value and unit . . . 26
1.3.2 Assess the risk of an individual threat . . . 27
1.4 Defense in depth . . . 28
1.4.1 Introduction . . . 28
1.4.2 Purpose . . . 28
1.4.3 Defense in depth vs. hardening . . . 28
1.4.4 Responsibilities . . . 29
1.4.5 Defense in depth example . . . 29
1.5 Developing a mitigation strategy . . . 31
1.5.1 Assess the efficiency of an individual mitigation measure . . . 31
1.5.2 Mitigation efficiency value and unit . . . 32
1.5.3 Alternatives to mitigation . . . 32
1.6 Criticality assessment and mitigation strategies . . . 34
1.6.1 Mitigation calculation . . . 34
1.6.2 Combining threat risk and mitigation efficiency . . . 34
1.6.3 Recommended mitigation strategies . . . 35
1.6.4 Residual risk . . . 35
1.6.5 Security viewpoints: binary or continuous values . . . 35
1.7 Cryptographic key and password basics . . . 37
1.7.1 Cryptographic key policies . . . 37
1.7.2 Password and cryptographic key comparison . . . 38

1.8 Impact of the system life cycle on the device life cycle . . . 39
1.8.1 VLAN plan . . . 39
1.9 Impact of device requirements on system planning . . . 40
1.9.1 Planning a secure installation location . . . 40
1.9.2 Planning for device availability . . . 41
1.9.3 Planning for Software auto update from the external memory . . . 41
1.9.4 Planning for SSH key auto upload from the External Memory . . . 41
1.9.5 Planning the Configuration load priority for the external memory . . . 41
1.9.6 Planning for signal contact use . . . 42
1.9.7 Planning for device and port LED visibility . . . 42
1.9.8 Planning how to check the security seal . . . 42
1.9.9 Planning restrictions to the device hardware interfaces . . . 43
1.9.10 Planning a secure boot policy <SL-C2> . . . 43
1.9.11 Planning a dedicated user account login policy . . . 44
1.9.12 Planning a dedicated user account password policy . . . 45
1.9.13 Planning a dedicated user account name and access role policy for device management . . . 46
1.9.14 Planning configuration encryption and the associated password . . . 48
1.9.15 Planning session timeouts <SL-C2> . . . 48
1.9.16 Planning a dedicated logging policy . . . 48
1.9.17 Planning a dedicated LLDP policy <SL-C2> . . . 49
1.9.18 VLAN plan considerations depending on redundancy protocols . . . 49
1.9.19 Advanced authentication measures <SL-C2> . . . 50
1.10 Impact of network aspects on system planning . . . 51
1.10.1 External server considerations . . . 51
1.10.2 Software update and configuration server considerations <SL-C2> . . . 51
1.10.3 External DHCP server considerations . . . 52
1.10.4 DNS server considerations . . . 53
1.10.5 Network time synchronization considerations <SL-C2> . . . 53
1.10.6 Authentication server considerations <SL-C2> . . . 53
1.10.7 Logging server considerations <SL-C2> . . . 54
1.10.8 eMail logging server considerations <SL-C2> . . . 55
1.10.9 Certificate and revocation management for authentication, logging and eMail servers <SL-C2> 55
1.11 Device-related policies . . . 57
1.11.1 Develop a backup policy for device-related data . . . 57
1.11.2 Develop a policy for replacing the device hardware . . . 57
1.11.3 Develop a policy for device hardware repair . . . 57
1.11.4 Develop a policy for device hardware decommissioning . . . 58
1.11.5 Develop a policy for device hardware disposal . . . 59
1.12 Operation and maintenance policy . . . 60
1.13 Document the planned policies . . . 61

2 Device security in the life cycle phases . . . 63
2.1 Develop the device configuration . . . 63
2.2 Software vs. hardware measures (logical vs. physical) . . . 64
2.3 Security-related vs. general device functions . . . 65
2.4 Prerequisites for installation and setup . . . 66
2.4.1 Possible further prerequisites . . . 66
2.5 Suggested installation step sequence . . . 67
2.5.1 Reasons for the suggested installation step sequence . . . 67
2.5.2 Suggested preparation for installation . . . 67
2.6 Choosing a secure installation location . . . 69
2.6.1 Considering the device availability requirements . . . 69
2.7 Considering the power supply redundancy requirements . . . 70

2.8 Considering the power budget requirements . . . 71
2.9 Considering the data link redundancy requirements . . . 72
2.10 Software update . . . 73
2.10.1 Initial access to the device management . . . 73
2.10.2 Initial password considerations . . . 73
2.10.3 Software update server considerations . . . 74
2.10.4 Secure boot considerations . . . 74
2.10.5 Best practices . . . 75
2.10.6 Detailed documentation . . . 75
2.11 Security setup overview . . . 76
2.11.1 Assign IP address parameters to the device management . . . 78
2.11.2 Disable HiDiscovery access . . . 78
2.11.3 Enable the secure boot mode <SL-C2> . . . 79
2.11.4 Enable configuration encryption <SL-C2> . . . 79
2.11.5 Set up a VLAN dedicated to device management access . . . 80
2.11.6 Disable logical access to the signal contact . . . 80
2.11.7 Disable logical access to unused ports and SFP slots . . . 81
2.11.8 Disable logical access for empty or unused media modules slots . . . 81
2.11.9 Disable the automatic device software update from the external memory (ACA) . . . 81
2.11.10 Disable the SSH key auto upload from the external memory . . . 81
2.11.11 Disable the Configuration load priority for the external memory . . . 82
2.11.12 Disable copying a software file into the device that lacks a valid cryptographic signature . . . 82
2.11.13 Disable writing an unencrypted configuration profile to the external memory (ACA) . . . 83
2.11.14 Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2> . 83
2.11.15 Disable insecure management protocols . . . 83
2.11.16 Set up management IP access restrictions . . . 84
2.11.17 Set up a dedicated HTTPS certificate for the device . . . 84
2.11.18 Set up a dedicated SSH host key for the device . . . 85
2.11.19 Set up the SSH Known Hosts fingerprints in the device . . . 86
2.11.20 Set up a dedicated user account login policy . . . 86
2.11.21 Set up a dedicated user account password policy . . . 87
2.11.22 Set up dedicated user account names and access roles for device management <SL-C2> . . . 88
2.11.23 Specify finite session timeouts <SL-C2> . . . 90
2.11.24 Set up time synchronization for the device clock <SL-C2> . . . 90
2.11.25 Set up certificates and possible revocation lists for authentication, logging and eMail servers . . . 91
2.11.26 Set up logging . . . 92
2.11.27 Disable SNMPv1/v2 write access . . . 92
2.11.28 Disable SNMPv1 traps . . . 93
2.11.29 Enable SNMPv3 traps . . . 93
2.11.30 Set up dedicated login banners . . . 93
2.11.31 Set up the DNS client functions . . . 94
2.11.32 Advanced: Access to the system monitor through the serial port . . . 94
2.11.33 Advanced: disable access to the CLI service shell . . . 94
2.11.34 Set up advanced user authentication <SL-C2> . . . 95
2.11.35 Create a backup of the device-related data . . . 96
2.12 Possible restrictions to the device’s hardware interfaces . . . 97
2.12.1 Restrict physical access to the SD card slot . . . 97
2.12.2 Restrict physical access to the USB port . . . 98
2.12.3 Restrict physical access to network ports or SFP slots . . . 98
2.12.4 Restrict physical access to empty media module slots . . . 98
2.12.5 Restrict physical access to the signal contact . . . 98
2.12.6 Restrict physical (visual) access to the device LEDs and port LEDs . . . 98

2.13 Device installation . . . 99
2.13.1 Checking the security seal . . . 99
2.13.2 Data connections . . . 99
2.13.3 Signal contact considerations . . . 99
2.14 Operation . . . 100
2.15 Maintenance . . . 101
2.15.1 Check the security seal (regularly or triggered by an event) . . . 101
2.15.2 Software update . . . 101
2.15.3 Hardware changes . . . 101
2.15.4 Device hardware replacement . . . 102
2.15.5 Device hardware repair . . . 103
2.16 Device decommissioning . . . 105
2.16.1 Deletion of confidential data and secrets . . . 105
2.16.2 Reset to the delivery state . . . 105
2.16.3 Secure physical destruction of the device and its accessories . . . 106
2.16.4 Secure removal of device-related data from the administration environment . . . 106
2.16.5 Secure disposal of the device hardware . . . 106

3 Network security support . . . 107
3.1 Introduction . . . 107
3.1.1 Prerequisites for setting up network security . . . 107
3.1.2 Deploying defense in depth for your network . . . 108
3.1.3 Harden your network . . . 108
3.2 Measures to help secure the network . . . 109
3.3 Restrict logical access to your network . . . 110
3.3.1 Set up VLANs for traffic segregation . . . 110
3.3.2 Disable GVRP and MVRP . . . 110
3.3.3 Set up the Port Security . . . 110
3.3.4 Set up DHCP Snooping . . . 111
3.3.5 Set up IP Source Guard . . . 111
3.3.6 Set up Dynamic ARP Inspection . . . 112
3.3.7 Set up the MAC authentication bypass . . . 112
3.4 Help secure the network protocols used . . . 114
3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 114
3.5 Help secure the redundancy protocols used . . . 115
3.5.1 Set up RSTP guards and helper protocols . . . 115
3.5.2 Set up the MRP (Media Redundancy Protocol) parameters . . . 116
3.5.3 Set Up MRP over LAG . . . 116
3.5.4 Set up Sub Ring with LAG . . . 116
3.5.5 Set up the HIPER Ring parameters . . . 116
3.5.6 Set Up HIPER Ring over LAG . . . 117
3.5.7 Set up the Redundant Coupling Protocol parameters . . . 117
3.5.8 Set up Ring/Network Coupling parameters . . . 117
3.6 Set up the attack protection support functions . . . 118
3.6.1 Set up the Denial of Service (DoS) parameters . . . 118
3.6.2 Set up the rate limiter . . . 118
3.6.3 Set up the Management MAC address conflict detection . . . 118
3.7 Set up Access Control Lists (ACLs) . . . 119
3.7.1 Introduction . . . 119
3.7.2 Resolving potential conflicts of aims for an ACL . . . 120
3.7.3 Creating ACLs and associations . . . 121
3.8 Set up the network time synchronization parameters <SL-C2> . . . 123

3.9 Set up the logging parameters . . . 124
3.9.1 Audit trail (created by persistent logging) . . . 124
3.10 Set up the LLDP parameters <SL-C2> . . . 125

A Security seal . . . 127
A.1 Overview . . . 127
A.2 Details . . . 128
A.2.1 Glued front label . . . 128
A.2.2 Potted device . . . 129
A.2.3 Security stickers . . . 129

B Password strength and policy guide . . . 131
B.1 Password classes . . . 131
B.2 Password policies . . . 133
B.3 Password schemes . . . 134
B.4 Password attack strategies . . . 135
B.5 Basic security assumptions . . . 136
B.5.1 Aggressive assumptions about attackers . . . 136
B.5.2 Conservative assumptions about users . . . 136
B.5.3 Conservative assumptions about the attack context . . . 137
B.6 Quantitative password strength . . . 138
B.6.1 High-complexity passwords . . . 138
B.6.2 Low-complexity passwords . . . 140
B.7 Attack resistance time (quantitative) . . . 143
B.7.1 Examples, unmitigated attack rate . . . 144
B.7.2 Attack rate mitigation . . . 144
B.7.3 Examples, mitigated attack rate . . . 145
B.8 Required attack resistance time (quantitative) . . . 146
B.9 Password entropy . . . 147
B.10 Calculating the required password entropy . . . 148
B.11 Password policy lookup tables (quantitative) . . . 150
B.11.1 Password entropy lookup tables . . . 150
B.11.2 Password policy lookup table, low-complexity passwords . . . 151
B.11.3 Password policy lookup table, high-complexity passwords . . . 152

C Considerations for manually entered keys . . . 155
C.1 Quantitative key strength . . . 155
C.1.1 Key entry as ASCII string . . . 156
C.1.2 Key entry as hexadecimal string . . . 157
C.1.3 Conclusion . . . 158
C.1.4 Example of random key value generation (tool use) . . . 160

D Index . . . 161

E Technical support . . . 175

F Readers' Comments . . . 176

Safety instructions

⚠ WARNING

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.

Safety information

⚠ WARNING
WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

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 “Device Security and Network Security Support” user manual contains an introduction, considerations for system security planning, and policy development, and an enumeration of device security measures. It also suggests how a secured device can assist in both securing and improving the availability of your network. Furthermore, password strength and specific mitigation measures are discussed, completed with a guide to password policy.

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:

• Item – Sub-item ▶ Item	General list item Sublist item Parameter value item
☐	Work or planning step
	Marks a reference to an external user or reference manual.
	The delivery state of the setting preceding the icon may be considered insecure.
Link	Cross-reference with link
Note:	A note emphasizes a significant fact or draws your attention to a dependency.
Boldface	Marks a key concept introduced for the first time.
"Chapter 1 > Chapter 1.1"	Practical reference to a chapter and sub-chapter in an external user manual or reference manual
[CR…][1]	Formal reference to an IEC 62443-4-2 Component Requirement
[CR… - informational][1]	Informational reference to an IEC 62443-4-2 Component Requirement
[CR…RE…][1]	Formal reference to the Requirement Enhancement of an IEC 62443-4-2 Component Requirement
[CR…RE…][1]	Formal reference to the Requirement Enhancement of an IEC 62443-4-2 Component Requirement
[NDR…][1]	Formal reference to an IEC 62443-4-2 Network Device Requirement
<SL-C…>[2]	Formally marks content that relates to IEC 62443 Security Capability Level 2 (SL-C2) or higher. For example, <SL-C2> marks content that conforms to SL-C2.
[SR…][1]	Reference to an IEC 62443-3-3 System Requirement
[SR… RE…][1]	Formal reference to the Requirement Enhancement of an IEC 62443-3-3 System Requirement

1. If a formal reference to the standard appears at the beginning of a chapter, it applies to the whole chapter. If a reference appears at the beginning of a paragraph or list item, it applies only to the respective paragraph or list item. If a reference appears in a comma-separated list, it applies only to the item tagged with the reference.
2. If a formal reference to the SL-C level appears at the end of the of a chapter headline, it applies to the whole chapter. If a reference appears at the end of a sentence (before the period), it applies only to the respective sentence.

Synopsis

This document deals with how to achieve and improve the security of an industrial communication network using the IEC 62443 "Security of Industrial Automation and Control Systems" series of standards as a framework.

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). SL-C1 means protection against casual or coincidental access by unauthenticated entities. Content conforming to SL-C1 is not marked up. However, content conforming to SL-C2 is marked up with <SL-C2>.

The chapter "Security Planning" (see on page 15 “Security planning”) introduces the subject, describes required preparatory work, explains some key concepts, and gives a hierarchy of hardware and software measures. It also describes the interdependence of device, network and system requirements, and details the required planning steps, resulting in a collection of policies.

The chapter "Device security in the life cycle phases" (see on page 63 “Device security in the life cycle phases”) details particular measures and steps to help secure a network device, based on the policies developed in the planning chapter.

The chapter "Network security support" (see on page 107 “Network security support”) describes particular measures to set up a network device to help support the security and availability of the network. The prerequisite is that the device itself has been secured. ACL setup is described extensively.

The appendix "Security seal" (see on page 127 “Security seal”) deals with the mechanical security methods of the device, their security properties, signs of tampering, the recommended procedures for checking the seals, and the recommended decommissioning procedure.

The appendix "Password strength and policy guide" (see on page 131 “Password strength and policy guide”) (informational only) deals with password strength, explains key concepts like password classes, password policies, password schemes, the strengths and weaknesses of password classes, shows how to calculate and improve the provided attack resistance time, shows how to calculate the required password entropy for an effective mitigation, and finally offers to look up a password policy that satisfies the desired level of attack resistance.

The appendix "Considerations for manually entered keys" (see on page 155 “Considerations for manually entered keys”) (informational only) deals with keys for symmetric cryptography, explains concepts like key classes, entry schemes, key strength, and the residual weaknesses of keys.

Audience

This security user manual primarily addresses Ethernet network planners, commissioners, administrators, operators, maintainers, and decommissioners.

The contents may also be useful for solution providers, sales partners, and system integrators.

1 Security planning

1.1 Basics

If you are new to security for industrial networks, you may find this chapter a good start.

1.1.1 Security terminology

The term "Security" typically can be subdivided into the following aspects.

Table 1: Aspects of security

Aspect	Description
Confidentiality	Only authorized entities have read access to specified information or devices.
Integrity	Only authorized entities have write or modify access to specified information. For devices, only authorized entities have the privileges to set up specified devices, and to install or update device software.
Availability[1]	Only authorized entities have the privileges to delete, modify, or deny access to specified information, or to remove or disable specified devices.
Authenticity	Specified information contains proof of which entity created or modified the specified information, or which entity installed, set up or a updated specified device.
Nonrepudiability[2]	Authenticated information or devices can be traced to the entity that created or modified the information, or updated or set up a device. This entity then cannot plausibly deny its creatorship.

1. Availability can be regarded as a part of integrity.
2. Nonrepudiability can be regarded as a part of authenticity.

Note:
Depending on your actual situation, some or all of the above aspects must be satisfied to consider a situation secure.

Example for confidentiality and integrity

For management of the device, the device offers different user account roles. These roles offer different degrees of access. This helps control confidentiality and integrity.

Table 2: Example for confidentiality and integrity, based on user account roles

User account role	Description	Security consequences
`unauthorized`	A user with this account role cannot log into the device.	Device management data remains confidential and integer.
`guest`	A user with this account role can log into the device to read data, except the audit trail. The user does not have write access to any data.	This user account role can read confidential data. Integrity is provided by read-only access.
`auditor`	A user with this account role can log into the device to read data, including the audit trail. The user can write the audit trail to a log file.	This user role can read confidential data. Integrity is provided by the immutable audit trail in the device.
`operator`	A user with this account role can log into the device to read and write device management data. Access to security-relevant settings and the audit trail is read-only.	This user role can read and write confidential data. Integrity is provided by read-only access to security settings and the immutable audit trail.
`administrator`	A user with this account role can log into the device to read and write data, including security-relevant settings. This role can also read the audit trail.	This user role can read and write confidential data. Integrity is provided by the immutable audit trail in the device

More terms

Most of the terms in the following table are used and explained in more detail in the remainder of this main chapter.

Table 3: Security terms

Aspect	Description
Vulnerability	A flaw or weakness of a system. Vulnerabilities can be unintentional (like an unintended software problem), or they can be unavoidable (like a system that offers a login). The union set of all vulnerabilities of a system is called an attack surface.
Threat	A potentially negative action, event, or circumstance that results in an unwanted impact to a system. A threat is related to a specific vulnerability of the system. A threat can be deliberate or accidental.
Threat model	A threat model is a model that defines the logical borders of a given asset, and the conditions under which threats are assumed. By defining these fundamental conditions, a threat model enables the reasonable, structured collection and description of perceivable threats. The outcome of a threat model is a threat collection.
Threat collection	A threat collection is the outcome when perceivable threats are applied to a threat model. It lists the perceivable threats that are deemed applicable to the threat model. It contains all collected threats, regardless of their exploitability, exploit severity, or their associated mitigation effort or effectiveness.
Threat profile	A threat profile is a threat collection ordered by threat risk, the combined treat/ mitigation criticality, or other, appropriate criteria.

Table 3: Security terms

Aspect	Description
Threat risk	The combination of both the degree of exploitability of a given threat and the severity of the results if the threat is applied to the system. The easier a threat can be exploited and the more severe its results, the higher the threat risk.
Mitigation	A process or action of countermeasure with the goal to thwart or attenuate a threat risk, either by lowering the exploitability of the threat or to diminish its results. Mitigation can be seen as part of vulnerability management.
Mitigation efficiency	The degree to which a given mitigation measure thwarts or attenuates a threat risk. It consists of the mitigation's effort and effectiveness. The lower the effort to implement a mitigation measure and the higher the effectiveness of the mitigation measure, the higher the mitigation effectiveness.
Criticality	The criticality applies to a specific threat risk in conjunction with a specific mitigation measure's efficiency. The higher the threat risk and the lower the associated mitigation's efficiency, the more critical this combination is.

1.1.2 Convenience vs. security: Navigating the field of tension

On a qualitative level (that is, not using a structured approach), the concepts of security and convenience are often seen as contradicting each other. As an example, consider a database that stores personal data, for example, of customers.

Convenience trumps security: If access to the database requires only one user name for any database user and requires only a trivial password for login:
- Such a system is convenient for the database users.
- At the same time, it is highly insecure because the confidentiality of the personal data is insufficient.

Security trumps convenience: If access to the database requires individual, hard-to-remember user names and enforces the use of system-generated, long and truly random passwords for login:
- Such a system is considerably inconvenient for the database users.
- At the same time, it can be regarded as highly secure because the confidentiality of the personal data is well protected.

In practice, often none of the above given extreme examples are feasible.

As a consequence, security planning needs an impartial approach, and should be based on metrics. This approach enables you to weigh threats against mitigation measures, helps you attain a reasonably secure system and also provides you with detailed, comprehensible points for your chosen mitigation measures.

Security is weighed against usability: If access to the database requires individual but short user names and allows memorable and user-chosen passwords according to an enforced password policy for login:
- This system can be seen as acceptable (convenient enough) for the database users.
- At the same time, it can be regarded as reasonably secure because the confidentiality of the personal data is appropriately protected.

Whitelist approach

In the context of network security, a whitelist approach is an implementation of the concept "Security trumps convenience", refined by the concept "Security is weighed against usability".

A whitelist approach means that only those network device functions shall be enabled that are clearly necessary for the network to function properly. All other device functions shall be disabled.

The functions that need to be disabled may include functions that are enabled in the factory setting, that is, in a device out-of-the-box. Therefore, plan a policy for the necessary functions.

1.1.3 Skepticism vs. optimism: qualitative security philosophy

When considering security aspects and the associated concepts of threat risks and mitigation efficiency, people can be associated with two groups:

- People with experience in security often tend to be conservative (skeptical), that is, they tend to give higher weight to security aspects and lower weight to convenience or usability aspects. The reason for that is that security considerations often involve examining seemingly uncritical details that can reveal unexpected threats, surprisingly high risks and unfortunately poor mitigation efficiency, possibly leading to the discovery of several critical, and as-yet, unmitigated vulnerabilities.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to higher security but can sometimes also lead to poorer convenience or even usability.
- On the other hand, people mainly concerned with usability and convenience, tend to be optimistic, that is, they focus on convenience while at the same time tend to overlook the security aspects of a system. The reason for that is that convenience considerations aim at minimizing the effort (for example, cognitive load) for a user which in turn can unintentionally create or exacerbate vulnerabilities (exploitable threats) in a system.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to good usability but can sometimes also lead to poor security.

As a consequence, a structured security approach that takes both aspects into account is indispensable.

1.1.4 Impartial assessment

To get an impartial overview over the security of a given or a planned system, an analysis is mandatory. This analysis typically consists of collecting the perceivable threats, based on a threat model, followed by an assessment of the individual threat risks.

This is typically followed by a collection and then an assessment of the available or perceivable mitigation measures.

The risk of a given threat can be combined with the efficiency of the respective mitigation. This combination can be regarded as a criticality value. This value can guide the priority with which a given threat/mitigation combination shall be pursued and also which mitigation strategy shall be employed.

1.1.5 Threat analysis

A thorough and reasonable security concept can only be developed when the threats to the asset under consideration are both known and assessed to a reasonable degree.

In practice, the threats are modeled and assessed in 2 steps:
- Develop a threat model that defines the conditions that in turn help collect and describe the conceivable threats to your system as completely as possible.
  The result is a threat collection.
- Develop a threat assessment concept that defines how to assess the collected threats individually and assign a risk to each threat.
  The result is a threat profile.

Note:
Without a threat model, the threat collection is prone to be incomplete, possibly leaving high-risk threats undiscovered.
Without a threat assessment, the threat profile, although possibly complete, is prone to assign unreasonable ad-hoc weight to individual threats. This may result in both high-risk threats going unmitigated as well as unreasonable effort going into the mitigation of minor threats. It also impairs the development of mitigation strategies.

1.1.6 Mitigation: confidentiality example

Confidentiality is often one of the most important aspects of security. It can be regarded as the property of a system or system component permitting or denying read access to an entity.

Confidentiality can be implemented by erecting one or more barriers for an unauthenticated entity. An unauthenticated entity must first identify and also authenticate itself toward a system that guards the confidential information. Only after the entity is regarded as authenticated, the system allows read access.

Typical mitigation measures (each implementing a barrier) can be:
- Compulsory identification (demanding a username).
- Compulsory authentication (demanding a password associated with the username).
- Measures that impede brute-force attacks, for example, by denying login access attempts for a given time after a number of successive failed login attempts.
- Possible additional measures to restrict login attempts to, for example, certain ports, VLANs, management protocols or IP source addresses.

As a consequence, develop an assessment for mitigation measures, and assign an efficiency to the individual mitigation measures in conjunction with the threat profile.

1.1.7 Theoretical and practical degrees of security

Even for barriers that provide a high degree of confidentiality, there are limitations:
- Theoretical confidentiality:
  - **Perfect confidentiality is unattainable.**
- Practical confidentiality:
  - **Near-perfect confidentiality can be uneconomical**, for example, if the cost for guarding the information is higher than the assigned price if the respective information is leaked.
  - **Near-perfect confidentiality can be impractical**, for example, if it requires device- and user-specific usernames and very long, truly random, device-specific passwords that users cannot reasonably memorize.

As a consequence, develop an assessment for the efficiency of an individual mitigation measure addressing a specific threat risk.

1.1.8 Strategies to provide improved security: confidentiality example

Regarding the above example, there are 2 aspects for achieving confidentiality:
- **Real-world barriers are imperfect**: No single real barrier offers perfect confidentiality.
- **Mitigation strategies may be required**:
  - **Defense in depth**: Single barriers can be combined (chained along the attacker's intended access path).
  - **Hardening**: Barriers (single or combined) can be implemented on several, parallel access paths, so a strong barrier cannot be circumvented by exploiting another, weaker, barrier.

As a consequence, develop an assessment for the criticality of a given threat risk in conjunction with the associated mitigation's efficiency. Also assess which critical thread risk/mitigation efficiency combinations need to be combined with other thread risk/mitigation combinations, for defense in depth. The resulting overview is also suitable for picking less critical thread risk/ mitigation efficiency combinations as possible targets for hardening.

1.1.9 Skepticism: Approximations in this document

In this document, approximations are sometimes used. The goal is to make the security considerations more practical and concise as opposed to a theoretical approach that may be more exact but impractical to implement.

When approximations are used, they typically tend to the skeptical side. That is, in case of doubt:
- Threat exploitability is considered easier (making the threat more likely).
- Threat exploit severity is considered higher (making a breach more dangerous).
- As a result, threat risks are considered higher.
- Mitigation effort is considered higher (making mitigation harder).
- Mitigation effectiveness is considered lower (making mitigation less worthwhile).
- As a result, mitigation efficiency is considered lower.
- The criticality (threat risk combined with mitigation efficiency) is considered more critical.

1.2 Overview

1.2.1 Subject

The "Security" user manual contains:
- Specific security considerations and actions to help secure your network device (see on page 63 “Device security in the life cycle phases”)
- Specific security considerations and actions which enable a secured network device to help support and enhance the security and availability of your network (see on page 107 “Network security support”)

It deals with the following life cycle phases of your network device:
- Secure installation (see on page 67 “Suggested installation step sequence”)
- Secure setup (see on page 76 “Security setup overview”)
- Secure operation (see on page 100 “Operation”)
- Secure maintenance (see on page 101 “Maintenance”)
- Secure replacement (see on page 102 “Device hardware replacement”)
- Secure repair (see on page 103 “Device hardware repair”)
- Secure decommissioning (see on page 105 “Device decommissioning”)

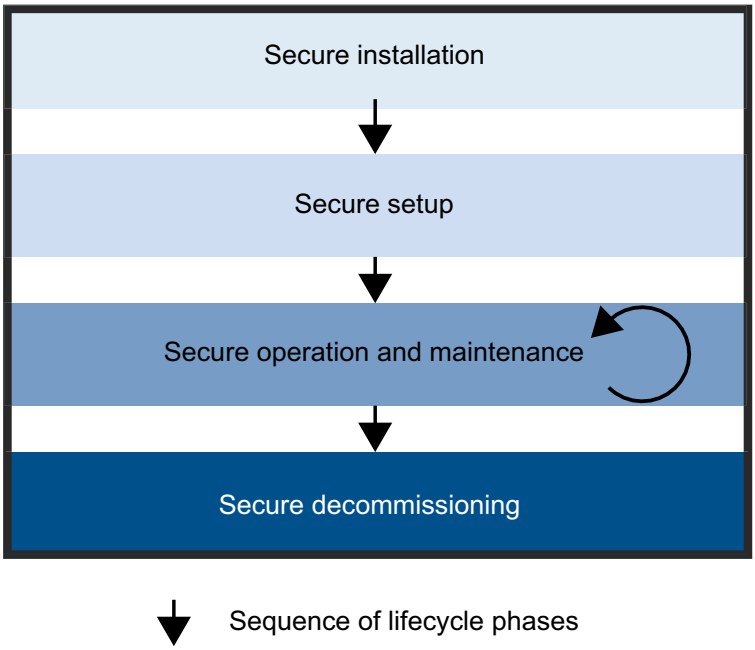


Figure 1: Device life cycle overview

1.2.2 Scope

This document deals with device security measures throughout the device life cycle. These measures build the base for the following overarching concepts:
- Security planning:
  - Assessing the threat risk, the mitigation efficiency, and the resulting criticality
  - Defense in depth for the device
  - Hardening the device

- Device security in the life cycle phases:
  - Specifically set up and deploy the device to help achieve defense in depth for your system
  - Specifically set up and deploy the device to help harden your system
- Network security support:
  - Specifically set up and deploy the device to support the security and availability of your network

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system life cycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system life cycle are made only if necessary, and only for information purposes.

Note:
For your network, additional planning and implementation steps may be required. For example, you may need a Layer 3 (L3) network plan in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

1.2.3 Capability security levels

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). SL-C1 means protection against casual or coincidental access by unauthenticated entities. Content conforming to SL-C1 is not marked up.

Content conforming to SL-C2 or higher is marked up, for example, with <SL-C2>.

1.2.4 Required preparatory work

This manual focuses on the security measures for your network device and how a secured device can help maintain the security and availability of your system.

To be effective, these measures need a solid base. The prerequisite for working through this manual is that you have already performed the required high-level security planning steps.

These planning steps may include:
- ☐ Research standards that are applicable to your situation, for example, IEC 62443.
- ☐ Define your system scope.
- ☐ Define the security zones in your system.
- ☐ Define the required subsystem and device functions in each zone.
- ☐ Compile the threats to the individual system zones.
- ☐ Assess the threats' properties (yielding the threats' risks).
- ☐ Compile a threat profile per zone.
- ☐ Contextualize your threat profile with regard to applicable standards.
- ☐ Collect mitigation measures (create a pool).
- ☐ Assess the mitigation measures' properties (yielding the mitigation measures' efficiencies).
- ☐ Associate the mitigation measures with the threat profile.
- ☐ Develop a mitigation strategy.
- ☐ Develop an overarching system security concept.
- ☐ Develop a defense in depth concept.
- ☐ Develop a hardening concept.

Note:
Depending on your circumstances, additional or different steps may be required.

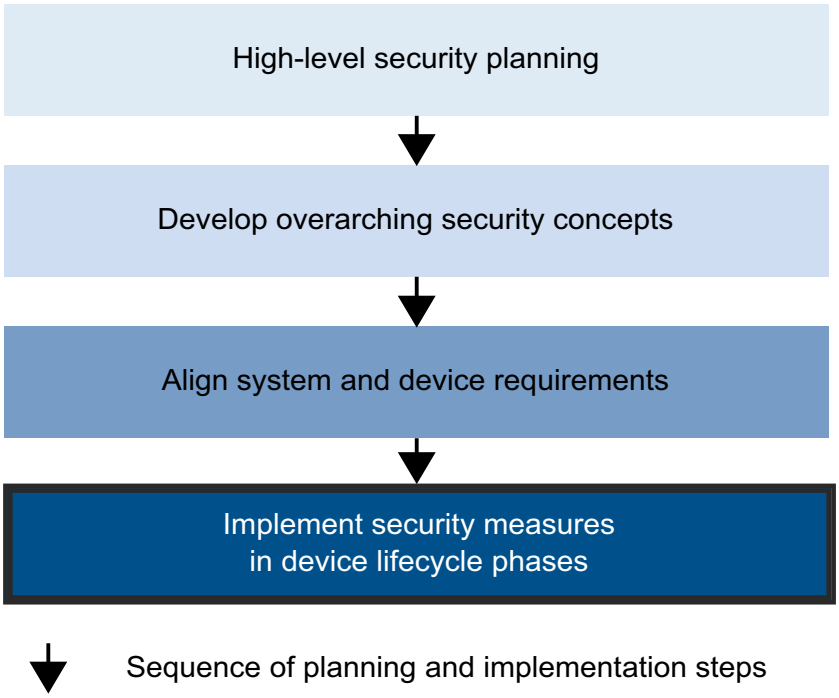


Figure 2: Required preparatory work hierarchy before implementation

The overarching system security concept may include:

Hardware-related concepts:
- [NDR3.13] Checking the security seal of a device
- A suitable physical location for the device
- Possible restrictions to the device's hardware interfaces
- A decommissioning policy [CR4.2]

Setup- (Software-) related concepts [CR7.6]:
- Concepts for helping secure the device itself:
  - A secure boot policy <SL-C2>
  - A user account login policy
  - A user account password policy
  - A user account and access role policy
  - A secure management protocol policy [CR7.7]
  - An SNMPv3 authentication and encryption types policy
  - An SNMPv3 trap password policy
  - A remote logging policy
  - A fall-back policy for protocols that offer fall-back
- Concepts for helping secure the network through device functions:
  - An LLDP policy <SL-C2>

Organizational concepts:
- Network time synchronization considerations <SL-C2>
- Software update and configuration server considerations <SL-C2>
- Certificate and revocation management for authentication, logging and eMail servers <SL-C2>
- Authentication server considerations <SL-C2>
- Logging server considerations <SL-C2>
- eMail logging server considerations <SL-C2>

- A backup policy for device-related data [SR7.3] [SR7.3 RE1] [CR7.3]
- A policy for device hardware replacement and repair [CR7.4]

Note:
This manual refers to individual overarching security concepts when required. However, the details of developing the security concepts themselves are outside the scope of this document.

1.2.5 Software setup scenarios and hardware scenarios

The software setup scenario consists of the required software setup steps. A particular software scenario typically has a specific hardware scenario as its base.

The hardware scenario consists of a secure installation location, and of possible device hardware interface access restrictions.

Note:
A hardware scenario can by itself help mitigate a considerable part of the threats.
The hardware scenario planning is required as a base for the software setup planning. A specific hardware scenario base can make the planning and deployment of the software setup steps significantly easier.
When planning device security, the hardware scenario is typically planned first, followed by the software setup scenario. The practical implementation sequence may deviate from the planning sequence.

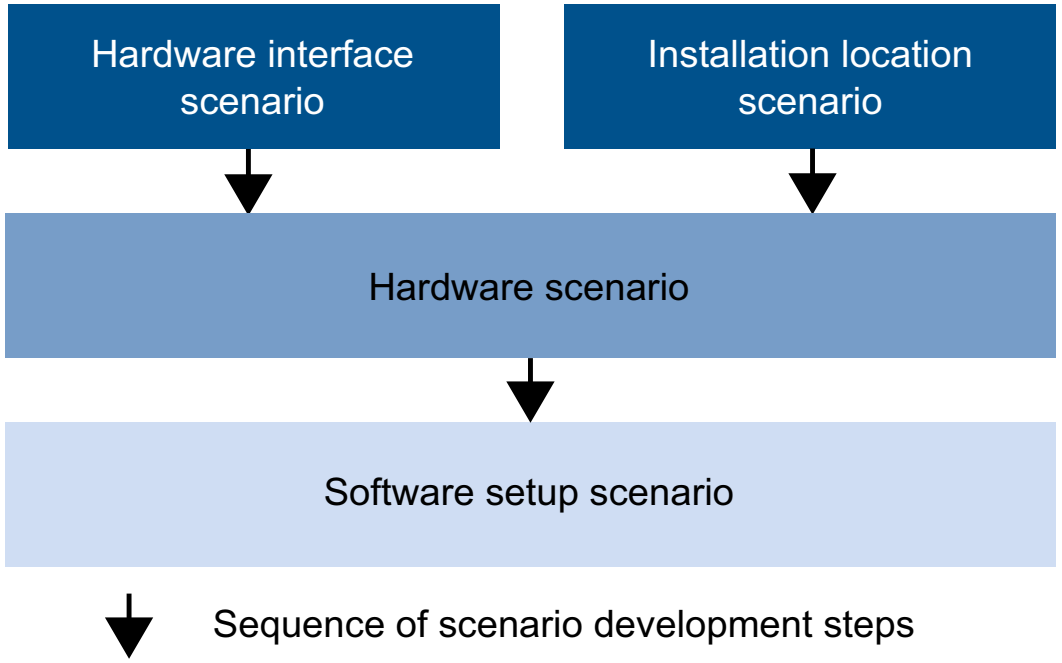


Figure 3: Basic scenario development steps

1.2.6 Scenario development

To develop a scenario (eventually represented by a set of hardware or software setup steps), typically a structured approach is taken. The steps of this approach are outlined in the following chapters:

- Gathering threats to compile a threat collection
- Assessing the threat risks to compile a threat profile
- Gathering mitigation measures to create a mitigation pool
- Assessing the mitigation measure efficiencies to develop a mitigation strategy
- Selecting mitigation measures for defense in depth
- Selecting mitigation measures for hardening

Consider using software tools that support you in these steps.

1.3 Compiling a threat profile

An individual threat profile for a device typically results from the specific user scenario (a collection of use cases) for the device.

The user scenario is defined by the following circumstances which are part of the threat model:
- the physical position of the device on the site
- the logical position of the device in the network
- the required functions of the device
- other functions of the device that are not required, but exist and may pose a vulnerability

When you compile the threat profile, determine the following aspects for each individual threat:
- Exploitability: How hard it is to exploit the individual threat
- Exploit severity: How significant the effects of an exploitation are

For gaining a better overview of the individual threats, you can assess the risk for an individual threat by combining exploitability and exploit severity.

1.3.1 Risk value and unit

A concrete, individual risk has a value and a unit:
- A risk can take on any positive, continuous, nonzero value.
- The unit of a risk depends on which risk you are considering. All risks include a probability (which has no unit) relating to a given time period (which has the unit of time). When combining these units, a risk has the unit of a rate, for example, a probability rate of 1% / year or 1 / 100 years.
  - Some risks can be reasonably associated with money, for example, the amount of money needed to restore lost data. Risks of this type, for example, can have the unit EUR / year, and an example value could be 10 EUR / year.
  - Other risks (for example, bodily injury or loss of reputation) cannot be assigned a straightforward amount of money. For risks of this type, it may be advisable to explicitly keep the unit of the individual risk together with the probability and the time period. For example, such a risk could have the unit "probability of light bodily injury per year" and an example value could be "probability of light bodily injury: 10 ppm / year".

Note:
The two types of risks (monetary and non-monetary) cannot be compared or combined directly because their units do not match. One possible approach to compare or combine them indirectly is to multiply the non-monetary residual risks by an explicit factor, resulting in a unit of money per time period. The factor should represent a very conservative approach to converting non-monetary risks (for example, personal injury) to monetary risks. This can be a demanding ethical assessment. There is no technical solution.

1.3.2 Assess the risk of an individual threat

The risk of a threat is determined both by its exploitability and by the severity of the effects of an exploit. These aspects can be summed up in a threat risk matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

Table 4: Threat risk matrix

	Exploitability		
Exploit severity	Easy	Medium-hard	Hard
High	**5**: Very high risk	4: High risk	**3**: Medium risk
Medium	**4**: High risk	**3**: Medium risk	2: Low risk
Low	**3**: Medium risk	**2**: Low risk	**1**: Very low risk

Note:
This matrix is intended to provide basic guidance on how to assess a threat's risk. Your actual situation may require a different assessment approach.

Table 5: Examples for threat exploitability

Threat	**Exploitability**	**Remarks**
Telnet access to the device management is possible.	Easy	Telnet offers no confidentiality, no integrity, and no authenticity.
SSH access to the device management has weak password.	Medium-hard	Dictionary or brute-force attack needed for exploit.
The device LEDS on front panel are visible.	Hard	An observer can infer a small part of the device and port status.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of threat exploitability.

Table 6: Examples for threat exploit severity

Threat	**Exploit severity**	**Remarks**
Attacker has access to the device management	High	Attacker can circumvent confidentiality, integrity and authenticity of sensitive information.
Attacker abuses a loop guard on a specific segment	Medium	Attacker can execute a Denial of Service (DoS) attack on this segment.
Attacker can create arbitrary Syslog messages	Low	Attacker can create false Syslog entries.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of exploit severity.

1.4 Defense in depth

1.4.1 Introduction

The concept of defense in depth is presented here because it is useful and even necessary for planning the mitigation strategies that are introduced later.

The same applies to the complementary concept of hardening.

1.4.2 Purpose

Defense in depth is a strategic concept that employs various independent security (that is, mitigation) measures to guard an asset under consideration against specific threats, as summed up in a threat profile.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

Note:
Implementing at least 2 barriers may require additional mitigation steps than those resulting from the particular user scenario part that the threat profile is based on. These additional mitigation steps could be taken from another part of the user scenario.
If no additional mitigation measures readily exist, this may be a sign that your user scenario or your mitigation strategy needs enhancement. You may then be required to plan for additional mitigation measures.

1.4.3 Defense in depth vs. hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as possible and reasonable. When you are planning a mitigation strategy, use the concept of defense in depth first and deduce a plan with particular mitigation measures. Then consider complementing the plan by using additional hardening measures.

Implementing hardening measures may also help to establish additional barriers in the context of defense in depth. This way, implementing hardening measures steps can also enhance the defense in depth measures. Therefore, hardening measures, although more general in nature, can be efficient.

A strategic approach to hardening may include the concepts:
- Least required privileges – for the device user accounts
- Least required device functions – for the device security
- Least required device functions – for the network security support

1.4.4 Responsibilities

Defense in depth and hardening both require planning, implementation, and maintenance. The system operator is responsible for performing these steps.

To help secure your system, consider the security measures provided in this manual. Select those that are most relevant for your specific situation.

1.4.5 Defense in depth example

An attacker is supposed to be connected to a company's industrial network. The asset under consideration is an industrial Ethernet switch in a production cell. The goal of the attacker is to gain access to the device management. The following graphic shows a possible arrangement of device-level barriers in a simplified way.

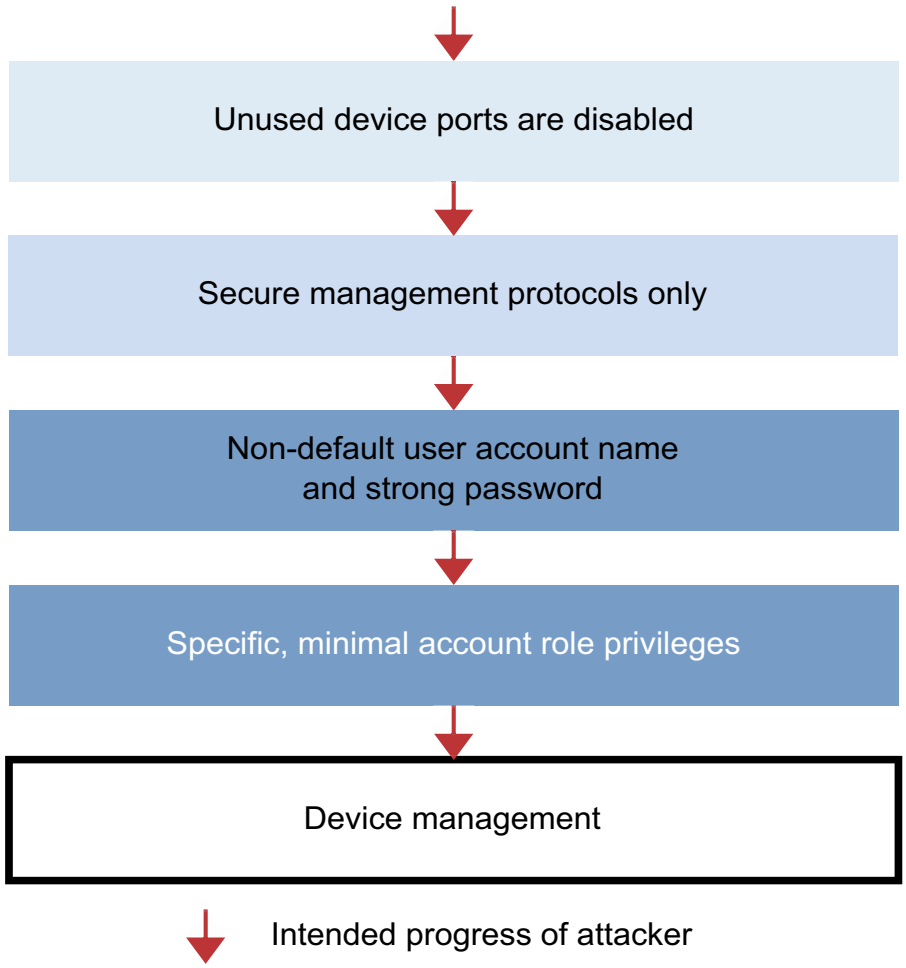


Figure 4: Barrier arrangement example for defense in depth

A more detailed example

The attacker is supposed to be connected to the company's industrial network (1). In more general cases, the attacker may instead be connected to the company Intranet (b) to the Internet (a).

Table 7: Defense in depth barriers example

ID	Barrier	Description
	System level	
a	Internet Firewall	The attacker must overcome the firewall between the Internet and the company Intranet to get access to the company Intranet.
b	Industrial Firewall	The attacker must overcome the industrial firewall to get access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
1	Dedicated device management VLAN	The attacker must overcome VLAN restrictions to snoop or inject packets.
	Device level	
2	Secure management protocols only	The attacker must overcome encryption to snoop or create packet contents.
2a	Non-default user account name[1]	The attacker must perform a brute-force attack to find the real user account name.
2b	Strong password[2]	The attacker must perform a brute-force attack to find the real password.
3	Specific, restricted account privileges	To read privileged data or manipulate device settings, the attacker must perform a dictionary or brute-force attack to find the real administrator account credentials.

1. A dedicated user account name can be device-specific and could be intentionally chosen to be non-descriptive.
2. A password can be specific to a certain access protocol (for example HTTPS) and can also be device-specific.

1.5 Developing a mitigation strategy

To build a mitigation strategy, first develop a pool of conceivable mitigation measures. Then assess the mitigation measures' efficiencies to develop a mitigation strategy.

When you develop a mitigation strategy, determine the following aspects for each individual mitigation measure:

- Effort: How much effort it takes to implement an individual mitigation measure
- Effectiveness: How effective the individual mitigation measure is in reducing or eliminating the threat

To gain a better overview on the individual mitigation measures, you can determine the efficiency for an individual mitigation measure by combining effort and effectiveness.

1.5.1 Assess the efficiency of an individual mitigation measure

The efficiency of a mitigation measure is determined both by the required mitigation effort and by the mitigation's effectiveness. These aspects can be summed up in a mitigation efficiency matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

Table 8: Mitigation efficiency matrix

	Effort		
Effectiveness	Small	Moderate	Big
High	**A**: Very high efficiency	**B**: High efficiency	**C**: High efficiency
Medium	**B**: High efficiency	**C**: Medium efficiency	**D**: Low efficiency
Low	**C**: Medium efficiency	**D**: Low efficiency	**E**: Very low efficiency

Note:
This matrix is intended to provide basic guidance on how to assess a mitigation measure's efficiency. Your actual situation may require a different assessment approach.

Table 9: Examples for mitigation efforts

Mitigation measure	Effort	Remarks
Disable Telnet access.	Small	Telnet access has a simple, binary, setting.
Set up restrictions to device management, by protocol and IP address range.	Moderate	The restrictions consist of a number of tabular settings and require an L3 network plan.
Create individual and CA-signed HTTPS certificates for each device.	Big	Generating private/public key pairs requires high-quality entropy and possibly dedicated hardware. Signing the individual keys by a certificate authority (CA) additionally requires a public key infrastructure (PKI).

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effort.

Table 10: Examples for mitigation effectiveness

Mitigation measure	Effectiveness	Remarks
Set the waiting period after a number of successive failed device management logins to >0.	High	The mitigated attack rate of a dictionary or a brute-force attack is significantly lowered.
Define a VLAN dedicated to device management access.	Medium	Flooded unknown unicast frames of the device management traffic are confined to the respective VLAN and cannot be intercepted from other VLANs.
Set up the CLI post-login banner with only the minimal information required.	Low	The restricted information applies to a situation when an attacker has already succeeded in logging in.

Note:
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effectiveness.

1.5.2 Mitigation efficiency value and unit

The efficiency of a concrete, individual mitigation measure can take on a value in the range $0 \leq x \leq 1$. It has no unit, so it can be regarded as a factor.

A very high mitigation efficiency means a value close to 1, and a very low mitigation efficiency means a value close to 0. In theory, a mitigation efficiency of 1 means that the individual mitigation measure completely eliminates the associated risk, and 0 means that the individual mitigation measure has no effect at all.

If we define the risk reduction factor as (1 - mitigation efficiency), we see that the greater the mitigation effectiveness, the smaller the risk mitigation factor.

1.5.3 Alternatives to mitigation

From a business-global view, there are alternatives to threat mitigation:

- **Risk acceptance:**
  - If the risk of a threat seems acceptable, a business may choose not to deploy any mitigation measures.
  - An example may be the leaking of unimportant data from a public system. The monetary risk of such a leak may be considered much lower than the monetary effort to secure the public system. As a consequence, a business may chose to accept the risk.
  - In this document, the acceptance of a risk is implicitly dealt with when considering the residual risk. If the risk of an unmitigated threat is lower than the accepted risk, the threat may be considered as acceptable.

- **Risk avoidance:**
  - If a business process that has a risk associated can be avoided, the risk is also avoided. In terms of technical systems, this translates into not setting up certain network or device functions.
  - An example may be that an internal system with business-critical data will not be connected to a public network but the subset of data intended to be publicly accessible is placed on another, dedicated system. The transfer of the publicly accessible data subset is then performed by a system that is only active while the transfer is performed. This avoids the permanent risk of leaking business-critical data from the internal system.
  - In this document, the avoidance of a risk is implicitly dealt with when excluding a device or network function from implementation because the risk cannot reasonably be mitigated.
- **Risk transference:**
  - In broad business terms, a certain business risk can be transferred to a third party.
  - An example can be buying insurance against the risk of fire in a data center. The risk of fire can never be completely ruled out, so it may reasonably to buy insurance.
  - Risk transference is outside the scope of this document.

Note:
This document focuses on technical mitigation measures, and does not detail the above alternatives to mitigation.

1.6 Criticality assessment and mitigation strategies

1.6.1 Mitigation calculation

Applying a concrete mitigation measure to counter an individual risk can be modeled by multiplying the risk value by the risk reduction factor (1 - mitigation efficiency), resulting in a smaller, residual risk.

If 2 or more mitigation measures to address the same risk are independent of each other (that is, they do not influence each other), the combined risk reduction factor can be calculated by multiplying the individual risk reduction factors. This is the numeric background of the general recommendation to combine mitigation measures if required or possible.

Note:
When you combine 2 or more mitigation measures to address the same risk, the mitigations may influence each other. That is, the risk reduction factor may be higher or lower than the calculation of the combined mitigation efficiency (1 - mitigation efficiency$_1$) × (1 - mitigation efficiency$_2$) would give.
Therefore, when you combine mitigation measures, check if you have to consider the combined mitigation efficiencies individually.

1.6.2 Combining threat risk and mitigation efficiency

The risk of an individual threat, combined with the efficiency of a specific mitigation measure, can be summed up in a criticality matrix. This matrix concentrates a 2-dimensional set of 25 possible combinations into a one-dimensional index of 9 values.

Table 11: Criticality matrix matrix (threat risk and mitigation efficiency combined)

	Threat risk				
Mitigation efficiency	**5**: Very high	**4**: High	**3**: Medium	**2**: Low	**1**: Very low
E: Very low efficiency	(1)	(2)	(3)	(4)	(5)
D: Low efficiency	(2)	(3)	(4)	(5)	(6)
C: Medium efficiency	(3)	(4)	(5)	(6)	(7)
B: High efficiency	(4)	(5)	(6)	(7)	(8)
A: Very high efficiency	(5)	(6)	(7)	(8)	(9)

Note:
This matrix is intended to provide basic guidance on how to assess the combination of a particular threat's risk with respect to a particular mitigation measure's efficiency. Your actual situation may require a different criticality assessment.

The criticality value is an index of the urgency of a given threat/mitigation combination. It can also be used to evaluate:
- The possible necessity for defense in depth
- Hints for possible hardening measures

1.6.3 Recommended mitigation strategies

Note:
The following table is intended to provide basic guidance on how to mitigate a given criticality (the combination of the threat risk and the mitigation efficiency).
You actual situation may require a different mitigation classification for any given criticality.
In fact, when assigning a mitigation strategy to a given criticality, you have considerable leeway to create a solution tailored to your situation.

Table 12: Criticality and recommended associated mitigation strategies

Criticality	Combination with another mitigation for the same threat
(1)	**Defense in depth required**: ≥2 other mitigation measures of same or higher efficiency
(2)	**Defense in depth required**: ≥1 other mitigation measure of same or higher efficiency
(3)	**Defense in depth required**: 1 other mitigation measure of same or higher efficiency
(4)	**Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency
(5)	**Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency
(6)	**Hardening recommended**: 1 other mitigation measure of same or higher efficiency
(7)	**Hardening recommended**: 1 other mitigation measure of same or higher efficiency
(8)	**Hardening optional**: 1 other mitigation measure
(9)	**Hardening optional**: 1 other mitigation measure

1.6.4 Residual risk

This residual risk per threat is the main outcome of the threat analysis and the applied mitigation strategy. The residual risk can take on any positive, nonzero value, that is, it is a continuous value.

Note:
For the unit of the residual risk, as well as how to combine different residual risk values (see on page 26 “Risk value and unit”)

1.6.5 Security viewpoints: binary or continuous values

The security of a system under consideration, with respect to a defined threat and defined circumstances (like operation and maintenance), can be viewed in two different ways:
- Security can be regarded as a continuous value (the residual risk can take on any value).
- Security can be regarded as a binary value (security is either given or not).

When viewed as a continuous value (derived from or identical to the residual risk), security can be improved gradually if the residual risk can be lowered.

When viewed as a binary value (security is either given or not), security is the result of comparing the residual risk to the maximum accepted risk for that given residual risk:
- Security is given if the residual risk is below or equal to the maximum accepted risk.
- Security is not given if the residual risk is higher than the maximum accepted risk.
- From this viewpoint, and strictly speaking, security, once given, cannot be improved.

Meaning of "improving the security"

When documents use phrases like "improving the security", this can have two meanings:
- For security as a continuous value, it means lowering the residual risk.
- For security as a binary value, it means having a secure system even after lowering the maximum accepted risk. This is typically achieved by lowering the residual risk.

In practice, a phrase like "improving the security" often has the meaning "lowering the residual risk".

1.7 Cryptographic key and password basics

The setup and operation of a network device typically involves the use of cryptographic keys and passwords.

An example of an asymmetric cryptographic key is:
- SSH server keys

Examples of passwords are:
- User account passwords
- SNMPv3 passwords
- The configuration encryption password
- User passwords for the Integrated Authentication Server (IAS)
- SNMPv3 trap passwords
- Passwords for eMail logging
- Passwords for a OPC UA connection

1.7.1 Cryptographic key policies

Cryptographic keys are used for two different types of cryptographic algorithms:
- Symmetric cryptographic algorithms
- Asymmetric cryptographic algorithms (also called public key algorithms)

The properties of symmetric and asymmetric algorithms are very different, and therefore, the properties of the respective keys are also different. This is why the recommended policies for generating the keys applies to different aspects:

Table 13: Comparison between symmetric and asymmetric cryptographic keys

Aspect	Symmetric cryptographic keys	Asymmetric cryptographic keys
Key properties	1 key (used for encryption as well as decryption)	2 keys (key pair): • Private key: – Must be kept secret – For decryption or signing • Public key: – Publicly available – For encryption or signature check
Key content	Essentially a large random number, need not be prime.	• Private key: 2 separate large prime numbers • Public key: Product of the private key's prime numbers
Typical key generation	Manually or automated (recommended)	Automated (compulsory)
Different key policy subjects	Key generation	Key signing
Common key policy subjects	Distribution, and rotation	Distribution, and rotation

For both cryptography types, this document gives general policy recommendations for key distribution and rotation.

For symmetric cryptography keys, this document also gives detailed policy recommendations for key generation (see the following chapter).

For asymmetric cryptography, the policy details for key generation and signing are outside the scope of this document.

1.7.2 Password and cryptographic key comparison

From a cryptographic viewpoint, symmetric cryptography keys can be considered a subset (special case) of passwords.

Note:
For asymmetric cryptography, the comparison between passwords and keys does not apply.

Table 14: Comparison between passwords and symmetric cryptographic keys

Property	Passwords	Symmetric cryptographic keys
Representation	ASCII string (in most cases)	• Hexadecimal • Base64-encoded • ASCII string
Length (representation)	Variable (allowed length range)	• Variable (allowed length range) • Fixed
Length (internal)	• Variable (when stored as value) • Fixed (when stored as hash)	Fixed
Creation	Manually by human users (in most cases)	• Automated, by dedicated software tools or systems • Manually by human users
Strength	Strength depends strongly on the enforced password policy. Without an enforced password policy, strength may be poor.	• Automated creation: High strength • Manual creation: Strength depends strongly on the enforced policy. Without a policy, strength may be poor.

For both passwords and symmetric cryptographic keys entered manually, their the strength depends strongly on the enforced policy. This is why a planning, setting up and enforcing a policy for manually generated passwords and keys is recommended. A policy may include the requirement that passwords or keys be generated by a specialized application.

For details on the strength of manually generated passwords (see on page 131 “Password strength and policy guide”).

For symmetric cryptographic keys, an automated generation is recommended. In cases where a key is entered manually, following a policy is highly recommended (see on page 155 “Considerations for manually entered keys”).

1.8 Impact of the system life cycle on the device life cycle

A network device is a component of the superordinate system. Therefore, the system life cycle determines parts of the device life cycle. A system life cycle involves a planning phase. The decisions taken in the planning phase affect the device life cycle directly or indirectly.

Typical decisions during system planning include:
- The physical location of the device, for example, its installation location and the location's environmental conditions
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

1.8.1 VLAN plan

[SR5.1] [CR5.1]

VLANs are a software-configurable concept to segregate a LAN (Layer 1) into separate Virtual LANs (VLANs) on Layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality and also helps reduce the network load on Layer 1.

A VLAN plan, including a dedicated device management VLAN, is considered a prerequisite for a secure setup of the device itself, and in turn for the security and availability of your system. Create a VLAN plan that segregates your network on Layer 2. A dedicated management VLAN can be a barrier component in the strategy "Defense in depth".

For small networks with few communication relations, a VLAN plan and the setup of VLANs may be considered unnecessary from a functional perspective. However, from a security perspective, VLANs can be useful or even required.

Note:
The redundancy protocols *HIPER Ring* and *Ring/Network Coupling* employ the fixed VLAN ID 1 for their protocol packets. If you intend to use these redundancy protocols, using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability (see on page 49 "VLAN plan considerations depending on redundancy protocols").

Note:
For your network, additional planning and implementation steps may be required. For example, you may need an L3 network plan in addition to the VLAN plan. Both the L3 network plan and the VLAN plan are outside the scope of this manual.

1.9 Impact of device requirements on system planning

Some requirements of the device have an impact on the system life cycle phases, in particular on system planning.

Topics of this interdependence include:
- A secure installation location, including the aspects:
  - Device availability: Power supply [SR7.5], and data link redundancy
  - Properties of the SD card slot
  - Properties of the USB port
  - Properties of the media module slots
  - Properties of the signal contact
  - Device and port LEDs
- The detailed physical device security requirements, in particular of its hardware interfaces
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the username and access role policy
  - For the SNMPv3 authentication and encryption type, and password policy
- Configuration encryption and the associated password
- VLAN ID restrictions arising from certain redundancy protocols: VLAN IDs ≥2 for payload traffic and device management
- Advanced user authentication measures like 802.1X, the MAC authentication bypass, a dedicated authentication policy list, LDAP or RADIUS or TACACS+: These measures require planning for the client in the device and may also require planning for external servers:
  - Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
  - Plan the MAC authentication bypass setup.
  - Plan the dedicated authentication policy list.
  - Plan the LDAP server setup.
  - Plan the RADIUS server setup.
  - Plan the TACACS+ server setup.

Note:
These topics are covered in more detail in the following main chapter (see on page 69 “Considering the device availability requirements”).

1.9.1 Planning a secure installation location

Select a location that in addition to its physical properties offers appropriate device security by restricting physical access to the device. For example:
- Install the device in a lockable room to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door.

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

1.9.2 Planning for device availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as required in your situation:

- [SR7.5] Provide a redundant power supply
- Provide an adequate power budget for the device
- Provide data link redundancy

1.9.3 Planning for Software auto update from the external memory

The device offers to automatically update the device software during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid software image in the root directory

Disabling the Software auto update from the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the Software auto update from the external memory (see on page 81 “Disable the automatic device software update from the external memory (ACA)”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to enable/disable the Software auto update.

1.9.4 Planning for SSH key auto upload from the External Memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid SSH key in the root directory

Disabling the SSH key auto upload from the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the SSH key auto upload from the external memory (see on page 81 “Disable the SSH key auto upload from the external memory”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to enable/disable the SSH key auto upload.

1.9.5 Planning the Configuration load priority for the external memory

The device offers to assign a priority for the loading of a configuration profile from the external memory.

Setting the Configuration load priority to *disable* for the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the Configuration load priority for the external memory (see on page 82 “Disable the Configuration load priority for the external memory”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to set the Configuration load priority for the external memory.

1.9.6 Planning for signal contact use

If you intend to use the signal contact, consider the following security aspects:
- To help protect the device, connect the signal contact only to a circuit that meets the device requirements.
- To help protect your system, connect the signal contact only to a circuit that does not have explicit security or safety requirements.

For details (see on page 80 “Disable logical access to the signal contact”).

Refer to the "Installation" user manual:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data > Signal contact" for allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

1.9.7 Planning for device and port LED visibility

The device and port LEDs show important information about the device state and the port states.

If you have high security requirements, consider the following security measures as required to help prevent information leakage:
- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the LEDs with a removable cover.

Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

1.9.8 Planning how to check the security seal

[NDR3.13]

<SL-C2> [NDR 3.11] [NDR 2.13]

Plan on how the security seal on a new device shall be checked (see on page 127 “Security seal”).

1.9.9 Planning restrictions to the device hardware interfaces

The possible modifications discussed here apply exclusively to the external hardware interfaces at the device surface. The intent of these measures is to restrict physical access to particular device hardware interfaces while keeping the device closed.

Plan the restrictions, like covering or obstructing a slot or a port, according to your requirements:
- Restrict physical access to the SD card slot.
- Restrict physical access to the USB port.
- Restrict physical access to network ports or SFP slots.
- Restrict physical access to empty media module slots.
- Restrict physical access to the signal contact.
- Restrict physical (visual) access to the device LEDs and port LEDs.

Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the hardware interfaces.

1.9.10 Planning a secure boot policy <SL-C2>

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The device offers booting only from trustworthy, that is, cryptographically signed software images that have not been tampered with.

Note:
The secure boot mode is required for a device setup compliant with SL-C2 and is the recommended boot mode.

The default setting of the secure boot mode is disabled . If the secure boot mode is disabled, the *Security Status* function in the Web-based interface notifies the user.

After the first successful boot from a proper, signed software image, you have the option to enable the secure boot mode. This initial boot process may have been taken place during manufacturing, or it may take place on the customer premises during a device software update.

Before you enable the secure boot mode:
- Check if the device is trustworthy, that is, that it has not been tampered with.
  For details on this check (see on page 127 “Security seal”) and the hardware installation manual.
- Make sure you are OK with using only secure boot-enabled software images in the future, that is, you will not need to downgrade to a non-secure boot-enabled software image.

Note:
Once you enable secure boot mode, you cannot disable it again. This means that the device will subsequently only boot from secure boot-enabled software images. Consequently the device will refuse booting from any other software images, including images of older device software releases even if these are perfectly intact and trustworthy but are not secure boot-enabled.

Upload of unsigned device software

When the secure boot mode is off, the device offers the possibility to upload an unsigned software image into the device. The default setting *Allow upload of unsigned device software* is enabled ⚠.

Note:
If you activate the secure boot mode, the device only accepts signed software images. The device no longer offers the possibility to upload an unsigned software image.

1.9.11 Planning a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

The device lets you set up a login policy for the user accounts.

The login policy applies consists of:
- Login attempts:
  The maximum number of failed user login attempts in a row until the device locks the respective user account
- Minimum password length:
  The minimum password length that the device enforces when changing a password or specifying a new password
- Login attempts period:
  The waiting time before the device auto-unlocks a locked user account

The login policy applies to every user account.

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Note:
For quantitative information on how to help ensure a secure login policy (see on page 144 “Attack rate mitigation”). For quantitative information on how to provide for hard-to-break passwords (see on page 131 “Password strength and policy guide”).

You can plan the following requirements for the user login:
- Login attempts:
  - For security reasons, plan the value as low as possible but >0.
  - For availability reasons, plan it as high as practical. Chose a value that fits your requirements.
- Minimum password length:
  - For security reasons, plan a value as high as reasonable.
  - Consider the type of password you want to use: High-complexity passwords contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords therefore should be considerably longer than high-complexity passwords.

  - Chose a minimum password length that fits your requirements.
  - For quantitative information on how to ensure hard-to-break passwords (see on page 131 “Password strength and policy guide”).
- Login attempts period:
  - For security reasons, plan the value >0 and as high as reasonable.
  - For availability reasons, plan it as low as practical but >0. Chose a value that fits your requirements.

Note:
Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port have an unlimited number of login attempts. These users are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.
To help secure your system, develop an overarching user account login policy.

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

1.9.12 Planning a dedicated user account password policy

[CR1.7]

The device lets you set up a password policy for the user accounts.

For detailed information on how to ensure hard-to-break passwords (see on page 131 “Password strength and policy guide”).

Consider the type of password you want to use (see on page 138 “Quantitative password strength”):
- High-complexity passwords have the following properties (see on page 138 “High-complexity passwords”):
  - No part of the password can be found in a dictionary
  - Contains ≥1 lowercase characters, ≥1 uppercase characters, ≥1 digits, and ≥1 special characters
- Low-complexity passwords have the following properties (see on page 140 “Low-complexity passwords”):
  - Consist of several words, each of which can be found in a dictionary
  - A punctuation character typically separates the words
  - Allow but do not require uppercase characters, digits, or special characters

High-complexity passwords of a given length contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords should be considerably longer than high-complexity passwords.

Note:
High-complexity passwords are more commonly used.

You can set up the following requirements for the password:
- The minimum number of uppercase characters
- The minimum number of lowercase characters

- The minimum number of digits
- The minimum number of special characters

Note:
The minimum password length belongs to the user account login policy (see on page 44 “Planning a dedicated user account login policy”).

To help secure your system, develop an overarching user account password policy. When you do, consider the following aspects to deter attackers:
- Consider using account names that are non-standard, and are non-descriptive to unauthorized entities.
- Consider using different user account names on different devices.
- Consider using different passwords on different devices, even for user accounts with the same name.
- Consider using different SNMPv3 passwords on different devices.

For the user credentials in the delivery state (see on page 86 “Set up a dedicated user account login policy”).

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

1.9.13 Planning a dedicated user account name and access role policy for device management

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

The device requires each user to identify themselves (by the user account name) and to authenticate themselves (by the associated password). The device associates a specific access role to each user account <SL-C2>.

Note:
User account names are case-sensitive.

Table 15: User account roles and privileges

User account role	Privileges
`unauthorized`	None: The device refuses login.
`guest`	The device permits reading of device management data, except the audit trail. The device refuses any write access to data.
`auditor`	The device permits reading of device management data, including the audit trail. The device permits writing the audit trail to a log file, but refuses any other write access.
`operator`	The device permits reading and writing of device management data. The device refuses write access to security-relevant settings and the audit trail.
`administrator`	The device permits reading and writing of device management data, including security-relevant settings. This device also permits the reading of the audit trail.

In the delivery state, the device has the following user account preconfigured:

Table 16: User credentials for the administrator account in the delivery state

Username	Password	User account role
admin	private (May have been changed at first login.)	administrator

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

Set up dedicated user accounts as required:

- Create user accounts with:
  - Dedicated names <SL-C2>
  - Chosen access roles that offer only the least required privileges
  - The password policy check enabled
- Assign the new user accounts strong, individual passwords.
  - Plan strong SNMPv3 authentication and encryption types and strong related passwords for the new user accounts.
- <SL-C2> Remove user accounts with standard names.

Note:
To help secure your system, develop an overarching user account and access role policy.
If you have high security requirements, consider planning different user account names and different passwords on different devices. Also consider user account names that are intentionally non-descriptive to unauthorized entities.
If you intend to use SNMPv3, also consider developing an overarching policy for SNMPv3 authentication and encryption types, and the related passwords. If you have high security requirements, consider planning different SNMPv3 passwords on different devices.

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

1.9.14 Planning configuration encryption and the associated password

Plan a configuration encryption policy:
- Plan if you want to enable the configuration encryption.
- Plan a specific password policy for the configuration encryption password.

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled ⚠. If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.

Note:
The configuration encryption password can and likely should be different from the user account passwords.
The configuration encryption password is not checked against the user account password policy.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/ Save" for the configuration encryption and the associated password.

1.9.15 Planning session timeouts <SL-C2>

Plan finite session timeouts for:
- The Graphical User Interface using HTTPS or HTTP
- The Command Line Interface through the serial port, SSH, or Telnet

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial port timeout function

1.9.16 Planning a dedicated logging policy

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

Set up the device logging settings:
- [CR2.11 RE1] Synchronize the device system clock to a trusted source <SL-C2>.
- Specify the severity levels of events you require to be logged.
- Specify the logging destinations you require, including possible remote logging.

To help secure your system, develop an overarching remote logging policy (see on page 54 “Logging server considerations <SL-C2>”).

Note:
The Syslog (system message logging) client in the device offers unencrypted communication as well as encrypted communication. To help secure your system, use encrypted Syslog, that is, Syslog over TLS <SL-C2>.
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device Syslog function.

1.9.17 Planning a dedicated LLDP policy <SL-C2>

When LLDP is enabled on your device:
- When the LLDP receive function is enabled, the device collects information about its neighbors and provides this information to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP send function enabled.
- When the LLDP send function is enabled, the device sends information about itself and its respective port to its neighbors. The neighbors can collect that information and provide it to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP receive function enabled.

LLDP can help automate a system inventory. LLDP may also help discover mismatches in port settings, like half-duplex and full-duplex settings, or VLAN settings, of ports connected to each other.

Depending on your security requirements, LLDP may need to be disabled on the device as well as on other network devices. You may also elect to enable only the receive function. The delivery state for LLDP is globally disabled.

For details (see on page 125 “Set up the LLDP parameters <SL-C2>”).

1.9.18 VLAN plan considerations depending on redundancy protocols

[SR5.1] [CR5.1]

Network availability can be an important base for the security of the superordinate system. The device offers redundancy protocols for this purpose.

The redundancy protocols *HIPER Ring* and *Ring/Network Coupling* employ the fixed VLAN ID 1 for their protocol packets. Using the VLAN ID 1 exclusively for these redundancy protocols can help enhance network availability. A VLAN plan (see on page 39 “VLAN plan”) that takes this particularity into account may require the use of VLAN IDs ≥2 for payload traffic and device management.

Note:
The other redundancy protocols, the Media Redundancy Protocol (MRP) and the *Redundant Coupling Protocol*, do not require a fixed VLAN ID to function. Therefore, MRP and the *Redundant Coupling Protocol* may be preferable over *HIPER Ring* and *Ring/Network Coupling*.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > *HIPER Ring*" for the *HIPER Ring* function
- Chapter "Switching > *Ring/Network Coupling*" for the *Ring/Network Coupling* function

1.9.19 Advanced authentication measures <SL-C2>

If you intend to use advanced user authentication measures like 802.1X, MAC authentication bypass or a dedicated authentication policy list:
- Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
- Plan the MAC authentication bypass setup.
- Plan the dedicated authentication policy list.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Network security > 802.1X" for the 802.1X function
- Chapter "Controlling the data traffic > MAC authentication bypass" for the MAC authentication bypass function
- Chapter "Device security > Authentication lists" for the dedicated authentication policy list

1.10 Impact of network aspects on system planning

1.10.1 External server considerations

<SL-C2> [CR 1.9]

To perform its functions, the device may rely on other system components. These system components are internal to the network but external to the device.

Typical examples are:
- Software update and configuration servers
- DHCP servers
- DNS servers
- Time servers
- Authentication servers
- Syslog servers

Using these servers can provide extended functionality that is not available in a purely local system concept. Examples for extended functionality are:
- Authentication servers offer various optional parameters, like assigning a VLAN ID to a user.
- Syslog servers offer log entry redundancy and virtually unlimited storage capacity.

For some protocols, like system message logging (Syslog), you can use the remote server in the normal state of operation, and have a fall-back to the local operation should the respective server become unreachable.

Note:
If your planned device configuration uses such external system components, consider developing an overarching policy for the external system components. This may include certificate and revocation management for authentication, logging and eMail servers.
If you intend to use a fall-back operation for a certain protocol, check if the protocol offers this possibility, and if it is appropriate for your situation. Then develop an overarching policy for the fall-back.

1.10.2 Software update and configuration server considerations <SL-C2>

If you intend to use servers for the update of the device software and to distribute device configuration files, plan a host key policy for these servers, possibly including server key rotation.

Note:
These keys typically are asymmetric cryptography keys.
As such, these keys need a specific key policy.
This policy is different than the policy for keys for symmetric cryptography that is discussed in other locations of this document.

Asymmetric key policy items may include:
- Plan a secure transfer protocol, for example, SFTP or SCP
- Plan the distribution of the server public key fingerprints
- Plan for a rotation of the server keys and the associated fingerprints

Note:
For authentication, logging, and eMail logging servers, trust is managed by another concept, TLS server certificates and revocations lists (see on page 55 “Certificate and revocation management for authentication, logging and eMail servers <SL-C2>”).

Server key rotation

Server key rotation on a regular basis limits the amount of data encrypted or signed by a specific key. This key can be:
- For asymmetric cryptography (used for example by TLS): The private key of a specific key pair
- For symmetric cryptography (used for example by encrypted SNMPv3 traps): The key that both communications partners share

Given that the key has a non-zero probability of being leaked, key rotation limits the amount of data encrypted or signed by that key:
- Data encrypted by that key may have also been leaked and might subsequently be exposed to decryption by the leaked key. Therefore, key rotation limits the extend of possible decryption exposure.
- For data signed by that key, it limits the amount of data that could have signed by an attacker, thus pretending a trustworthy signature.

Server key rotation means that a specific key will only be user for a limited period and will normally replaced by another key shortly before the period of the given key runs out.

A server key rotation scheme may include the setting up of 2 or more keys per server whose validity periods are adjacent or overlap.

1.10.3 External DHCP server considerations

If you intend to use DHCP to obtain the device management IP address or other parameters, plan the DHCP server setup. If you intend to use external DHCP servers, consider developing an overarching DHCP server policy.

Note:
The DHCP client implicitly trusts the DHCP server. Depending on your actual situation, assigning a static (that is, locally specified) IP address to the device may be considered more secure than using the DHCP client.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Basic settings > IPv4 > BOOT/DHCP" for the device IPv4 DHCP client function
- Chapter "Basic settings > IPv6 > DHCP" for the device IPv6 DHCP client function

1.10.4 DNS server considerations

If you intend to use the device DNS client functions that require an external DNS server, plan the DNS server setup. If you intend to use external DNS servers, consider developing an overarching DNS server policy.

Note:
The device's DNS client implicitly trusts the external DNS server. Depending on your actual situation, not using the device DNS client functions may be typically considered more secure than using an external DNS server.

Refer to the "Graphical User Interface" reference manual, chapter "Advanced > DNS > DNS client" for the device DNS client function.

1.10.5 Network time synchronization considerations <SL-C2>

[CR2.11 RE1]

Network time synchronization can be required for several reasons, including secure logging or TLS certificate validation.

The device offers SNTP and PTP for synchronizing its internal clock.

The time synchronization protocols SNTP and PTP implicitly trust their time source. To make network time synchronization more secure, consider developing an overarching network time synchronization policy.

Parameters of this policy may include:
- The choice of the network protocol for time distribution
- The choice of the primary time sources
- The choice of time synchronization paths, based on precision, availability, and security requirements
- Requirements for controlling or tuning the chosen network time protocol on the nodes that are part of the time synchronization path
- The choice of Multicast or Unicast packets on the network layer (L3)

Plan a suitable mitigation concept tailored to your threat model. For example, restrict the time sources a given device accepts. Based on your mitigation concept and your chosen policy, determine which settings are required for the individual devices.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

1.10.6 Authentication server considerations <SL-C2>

<SL-C2> [CR 1.9]

If you intend to use authentication servers to help the device authenticate users or other system entities, plan the setup of the appropriate authentication servers:
- Plan for the dedicated local authentication policy list to use an external authentication server.
- Plan the external LDAP server setup.

- Plan the external RADIUS server setup.
- Plan the external TACACS+ server setup.

Note:
Depending on your actual situation, setting up only a static, local Integrated Authentication Server (IAS) in the device may be considered more secure than using external authentication servers.
The LDAP client in the device offers encrypted communication as well as unencrypted communication. The default setting is unencrypted communication ⚠. To help secure your system, use encrypted LDAP communication. Secure LDAP establishes trust for the device (the LDAP client) towards the LDAP server by means of a TLS server certificate.
The RADIUS client in the device exclusively offers obfuscated communication. The secure RADIUS protocol establishes mutual trust between the device (the RADIUS client) and the RADIUS server by means of a shared secret.
The unsecured protocol versions of LDAP and RADIUS implicitly trust their servers. If you intend to use remote authentication, consider using developing an overarching remote authentication policy and using only encrypted LDAP or obfuscated RADIUS.

Note:
Encrypted LDAP can be considered preferable over obfuscated RADIUS or TACACS+ because encrypted LDAP employ newer and more sophisticated concepts for both establishing trust towards its authentication server and the encryption of the communication.
RADIUS and TACACS+ use obfuscated communication which offers weaker security than encrypted LDAP.

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device security > Authentication lists" for the dedicated authentication policy list
- Chapter "Device security > LDAP" for the device LDAP client function
- Chapter "Network security > RADIUS" for the device RADIUS client function
- Chapter "Network security > TACACS+" for the device TACACS+ client function

1.10.7 Logging server considerations <SL-C2>

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

If you intend to use Syslog (system message logging) servers to help keep a complete and persistent log of the events reported by the device, plan the setup of the appropriate external Syslog servers.

<SL-C2> [CR 1.9]

Note:
The Syslog client in the device offers unencrypted communication as well as encrypted communication. To help secure your system, use encrypted Syslog, that is, Syslog over TLS <SL-C2>. The encrypted Syslog protocol establishes trust for the device (the LDAP client) towards the LDAP server by means of a TLS server certificate.
Using Syslog servers offers the advantage of sending the log entries to a remote location different from the device. This helps provide redundancy. It also helps overcome local log capacity constraints on the device.

If you intend to use remote logging, consider developing an overarching remote logging policy and consider using only encrypted Syslog.
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > Syslog" for the device Syslog function
- Chapter "Diagnostics > Report > Audit trail" for the device Audit trail

1.10.8 eMail logging server considerations <SL-C2>

<SL-C2> [CR 1.9]

If you intend to use eMail servers to as part of your logging policy, plan the setup of the appropriate external eMail (SMTP) servers.

The eMail client in the device offers unencrypted communication as well as encrypted communication (SMTP over TLS). To help secure your system, use encrypted eMail submission <SL-C2>. Encrypted eMail submission establishes trust for the device (the eMail client) towards the eMail server by means of a TLS server certificate.

If you intend to use eMail logging, consider developing an overarching eMail logging policy and using only encrypted eMail submission.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Email notification" for the device eMail function.

1.10.9 Certificate and revocation management for authentication, logging and eMail servers <SL-C2>

<SL-C2> [CR 1.9]

If you intend to use TLS-based servers for one of the following functions, plan a policy for the management of the server certificates and revocation lists, possibly including server certificate rotation:
- Authentication servers (see on page 53 “Authentication server considerations <SL-C2>”)
- Logging servers (see on page 54 “Logging server considerations <SL-C2>”)
- eMail logging servers (see on page 55 “eMail logging server considerations <SL-C2>”)

Note:
For software update and configuration servers, trust is managed by another concept, SSH Known Host key fingerprints (see on page 51 “Software update and configuration server considerations <SL-C2>”).

Server certificate rotation

A TLS server certificate, issued by a Certificate Authority (CA) attests the validity and trustworthiness of a public key that was created and submitted for attestation by the server administrator. A certificate therefore implicitly attests the validity and trustworthiness of the private key associated with the signed public key.

Certificate rotation means that a specific certificate has an explicitly limited validity period and will normally be replaced by another certificate shortly before the validity period of the current certificate runs out.

Generating a new certificate includes generating a new key pair by the server administrator and attestation of the new public key by the CA. Certificate rotation therefore also requires key rotation, and the properties of the key rotation apply accordingly (see on page 52 “Server key rotation”).

A certificate rotation scheme may include:
- Setting up of 2 or more certificates per server
- The different certificates attest different public keys of the given server.
- The validity periods of these certificates overlap.

1.11 Device-related policies

1.11.1 Develop a backup policy for device-related data

[SR7.3] [SR7.3 RE1]

Consider developing a backup policy for device-related data. This minimizes your effort for replacing a device if the device becomes inoperable.

This policy may include:
- [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Creating a backup copy of the device configuration profiles <SL-C2>.
- Keeping the backup files separate from the device in a secure location.
  For example, placing the backup files on a file server in a device-specific folder.
- Including other device-specific data in the same device-specific folder.
  For example, including device-specific private keys or certificates.
- Using a file or folder numbering scheme or even a version control tool to track the device configuration history.

1.11.2 Develop a policy for replacing the device hardware

[CR7.4]

<SL-C2> [CR 1.9] [NDR 3.11] [NDR 2.13]

Consider developing a policy for replacing the device hardware.

Topics of this policy may include:
- Which data of the former device shall be backed up to a remote location
- [NDR3.13] How the security seal of the new device shall be checked (see on page 127 “Security seal”)
- Which data of the former device shall be restored to the new device. For example, the following data for the new device may or may not be identical to the former device’s data:
  - User account names and passwords
  - Host keys (public and private) or certificates
- Which software shall be loaded onto the new device. For example, the software on the new device may or may not be identical to the former device’s software:
  - The new device may be of a different device family.
  - The new device may be of a different device generation.
- If the hardware interfaces of the new device shall be restricted

Align the device hardware replacement policy with:
- The hardware repair policy
- The hardware decommissioning policy

1.11.3 Develop a policy for device hardware repair

<SL-C2> [CR 1.9]

Consider developing a policy for device hardware repair.

If a device needs repair, consider your actual confidentiality needs regarding the data present on the device:

- The configuration profiles and configuration scripts
- The boot parameters
- The current HTTPS certificate
- The current SSH host key or host key pair
- The current software files
- The configuration profiles on the external memory

Furthermore, consider the following organizational steps:

- For the device hardware, specify:
  - If you expect to get the same device back (identified by the same base MAC address)
  - If you agree to receive another device of identical type (will have a different base MAC address)
  - If you agree to receive a device of another, superior type or generation (will have a different base MAC address and possibly also other properties)
- For the security seal on the device (see on page 127 “Security seal”), specify
  - How you check the security seal’s condition before sending the device to the manufacturer
  - How you check the security seal’s condition after receiving the device back from the manufacturer

1.11.4 Develop a policy for device hardware decommissioning

Consider developing a policy for device hardware decommissioning.

Specify which of the following steps to carry out, and how.

Note:
Depending on your actual environment, fewer, more or other steps than those listed below may be necessary.

Deletion of confidential data and secrets:

- Reset to the delivery state:
  - Deletes the configuration profiles and configuration scripts in the device
  - Resets the boot parameters
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate
  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair
  - If the external memory is plugged in, the device also deletes the configuration profiles on the external memory.
- Possible secure wipe (instead or in addition to the reset to the delivery state):
  - Securely overwrite the data and secrets listed in the previous list item, "Reset to the delivery state".
  - If required, securely overwrite the software files in the device.
  - Securely overwrite every configuration profile on a connected external memory.

Secure physical destruction of the device and its accessories:
- Destroy the security seal on the device (see on page 127 “Security seal”).
- Physically destroy the device, including the flash memory chips. This destroys the data and secrets listed in the above list item "Reset to the delivery state".
- If required, physically destroy the external memory.

Note:
The reset to the delivery state leaves the audit trail intact.
The reset to the delivery state leaves the secure boot setting intact. <SL-C2>
If you intend to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

For the secure removal of device-related data from the administration environment, perform the following steps. This may include:
- The removal of:
  - Configuration data and its backups
  - Private cryptographic keys
  - Self-signed certificates
- The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

1.11.5 Develop a policy for device hardware disposal

Consider developing a policy for device hardware disposal.

If you have high security requirements, consider disposing of the device by shredding it.

1.12 Operation and maintenance policy

Develop a policy for operation and maintenance. Such a policy may include:

- Which administrative roles for operating or maintaining the device hardware are required
- Which administrative roles for operating or maintaining the device settings are required, along with specific privileges and responsibilities for each role (see on page 46 “Planning a dedicated user account name and access role policy for device management”).
- A schedule for routine operation and maintenance tasks
- A synchronization with operation or maintenance tasks for superordinate system components
- The extent of the scheduled tasks, for example:
  - Looking for a available software update and evaluating or applying it
  - Performing a check on a set of security-related settings and statuses
  - <SL-C2> [CR 1.9] Performing a server key or certificate rotation and applying the resulting changes to the associated device settings, possibly both before and after the server key or certificate rotation
- The extent of active measures that determine the device security status, like:
  - Checking the security status variable of the device
  - Checking other, selected security-related settings in the device
  - Regular penetration tests
- Manual triggers of an out-of-schedule operation or maintenance task, for example:
  - Because of a change in the device setup
  - Because of an audit
  - Because of the results of a penetration test
  - Because of the manual evaluation of log files
- Automatic triggers of an out-of-schedule operation or maintenance task, for example:
  - Caused by the detected change of the security status variable of the device
  - Caused by the detected change in selected security-related settings and statuses
  - Caused by the automatic evaluation of log files

1.13 Document the planned policies

Document the overarching policies. These policies serve as an essential base for planning the individual device configuration and setting up the device.

Depending on your requirements and circumstances, you can plan and maintain the policies with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated software tool.

2 Device security in the life cycle phases

2.1 Develop the device configuration

Based on your documented overarching policies, plan (develop) the configuration for each considered device. If you follow a whitelist approach, include the necessary function policy from your whitelist policy.

Document the planned configuration for each considered device. This helps to keep track of the system.

This planned configuration per device can be, for example:
- On a generalized level:
  The device needs to have 2 ring ports and 1 uplink port.
- On a concrete level:
  The device needs ports 3 and 4 as MRP ring ports with a data rate of at least 1 Gbit/s, and ports 1 and 2 for the redundant uplink with at least 100 Mbit/s.

Depending on your actual situation, you can either directly deduct the detailed device configuration from the policies, or allocate 2 steps by planning the device configuration on a generalized level first and then detailing it.
- For a small system or system zone, and if you have already decided which device types you will use, it may be appropriate to plan the concrete device configuration directly (deduct it directly from the policies).
- For a large or complex system or system zone, it may be necessary to split the steps:
  - Plan a generalized device configuration first.
  - Decide which concrete device type and variant you want to deploy.
  - Detail the device configuration.

Depending on your requirements and circumstances, you can plan and maintain the device configuration with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated network planning/management tool.

2.2 Software vs. hardware measures (logical vs. physical)

This main chapter deals with software setup measures as well as hardware measures.

- The software setup measures are also referred to as logical measures.
  - For example: Disable logical access to unused ports and SFP slots.
  - For example: Disable logical access to the digital input.
- The hardware measures are also referred to as physical measures.
  - For example: Restrict or disable physical access to the USB port or the SD card slot.
  - For example: Restrict or disable physical access to the SD card slot.

2.3 Security-related vs. general device functions

The software setup measures in this main chapter deal with the security-related setup of device functions throughout the life cycle phases of the device.

The device functions can be divided into three groups:

- Security-related device functions that help secure the device itself:
  The setup of these functions is described in this main chapter (see on page 76 “Security setup overview”).
- Security-related device functions that help secure your system and improve its availability:
  The setup of these functions is described in the following main chapter "Network security support" (see on page 107 “Network security support”).
- General device functions: The setup of the general device functions is outside the scope of this document. If you follow a whitelist approach, include the necessary function policy from your whitelist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.

  For the general device functions, refer to the detailed manuals:
  - The "Configuration" user manual
  - The "Graphical User Intere" user manual
  - The "Command Line Interface" reference manual
  - The "Installation" user manual (for hardware-related setup steps)

2.4 Prerequisites for installation and setup

The prerequisite for working through this section is that you have already performed the system planning steps, including:

- ☐ Planning a suitable physical location for the device (see on page 69 “Choosing a secure installation location”)
- ☐ Planning restrictions to the device hardware interfaces (see on page 43 “Planning restrictions to the device hardware interfaces”)
- ☐ If you follow a whitelist approach, develop a necessary function policy from your whitelist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.
- ☐ Developing a dedicated user account **login** policy (see on page 44 “Planning a dedicated user account login policy”)
- ☐ Developing a dedicated user account **password** policy (see on page 45 “Planning a dedicated user account password policy”)
- ☐ Developing a dedicated user account and access role policy for device management (see on page 46 “Planning a dedicated user account name and access role policy for device management”)
  - – Developing a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords
- ☐ Planning configuration encryption <SL-C2> (see on page 48 “Planning configuration encryption and the associated password”)
- ☐ Planning session timeouts <SL-C2> (see on page 48 “Planning session timeouts <SL-C2>”)
- ☐ Developing a dedicated logging policy, possibly including remote logging (see on page 48 “Planning a dedicated logging policy”)
- ☐ Developing a policy for the servers that hold device software updates and configuration files <SL-C2> (see on page 51 “Software update and configuration server considerations <SL-C2>”)
- ☐ Planning a dedicated LLDP policy <SL-C2> (see on page 49 “Planning a dedicated LLDP policy <SL-C2>”)

If required, the following organizational concepts are also part of the above planning work:

- ☐ Network time synchronization considerations <SL-C2>
- ☐ [CR 1.9] Certificate and revocation management for authentication, logging and eMail servers <SL-C2>
- ☐ Authentication server considerations <SL-C2>
- ☐ Logging server considerations <SL-C2>
- ☐ eMail logging server considerations <SL-C2>
- ☐ A backup policy for device-related data [SR7.3] [SR7.3 RE1]
- ☐ A policy for device hardware replacement

2.4.1 Possible further prerequisites

Your network may require further system planning steps, including:

- ☐ Traffic segregation on Layer 2 by a VLAN plan
- ☐ Use of a network management system like Industrial HiVision (optional)

Note:
The details of these steps are outside the scope of this document.

2.5 Suggested installation step sequence

The steps in the device security life cycle phases in a practical order are:

- ☐ Choose a secure installation location (see on page 69 “Choosing a secure installation location”)
- ☐ Perform the initial software update (see on page 73 “Software update”)
- ☐ Perform the initial security setup (see on page 76 “Security setup overview”)
- ☐ If required, modify the hardware interfaces for security (see on page 97 “Possible restrictions to the device’s hardware interfaces”)
- ☐ Perform the initial device installation (see on page 99 “Device installation”)
- ☐ Operation measures (see on page 100 “Operation”)
- ☐ Maintenance measures (see on page 101 “Maintenance”)
- ☐ Decommissioning measures (see on page 105 “Device decommissioning”)

Note:
Depending on your requirements, you may want to perform the steps in a different sequence.

2.5.1 Reasons for the suggested installation step sequence

Performing the initial setup and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, TLS server certificates, SSH known host fingerprints, prepared device configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be set up contiguously.
- For certain hardware measures like physically blocking the SD card slot, you may need the SD card slot for the initial setup and software update before you can block the SD card slot.
- For certain hardware measures like physically blocking a USB port, you may need the USB port for the software update and initial setup before you can block the USB port.
- The remaining work steps in the field require less time.

2.5.2 Suggested preparation for installation

The following suggested steps and their sequence can help reduce the initial effort and save time:

- ☐ Check the security seal of the device, (see on page 127 “Security seal”).
- ☐ Check the available device software release on the Hirschmann product pages on the Internet at catalog.belden.com.
- ☐ Decide which device software release you want to run on your devices.
- ☐ Download the respective software files.
- ☐ If you want to load the device configuration or update the device software from an SFTP or SCP server, determine the fingerprints of the respective configuration profile or software update servers. Verify that the fingerprints are from a trustworthy source, like the server administrator.

☐ If desired, prepare the individual device configuration files based on the respective planned device configuration. If you want to enable the configuration encryption, (see on page 79 “Options to enable configuration encryption”).
☐ Prepare the device labels.

Note:
To help keep your system secure, consider using the latest available release of the device software. If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the files (software or configuration files) are cryptographically signed.

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

Refer to the "Configuration" user manual:
- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

2.6 Choosing a secure installation location

Note:
The prerequisite for working through this section is that you have already performed the planning for a secure installation location (see on page 40 “Planning a secure installation location”).

Select an installation location that in addition to its physical ambient conditions offers appropriate device security by restricting physical access to the device or its hardware interfaces.

Check that the following device security requirements are fulfilled as required:
- Install the device in a room that can be locked and to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door (see on page 98 “Restrict physical (visual) access to the device LEDs and port LEDs”).

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

2.6.1 Considering the device availability requirements

Device availability can be an important base for the security of the superordinate system. Therefore, also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled, if required:
- [SR7.5] Consider the power supply requirements (see on page 70 “Considering the power supply redundancy requirements”).
- Consider the power budget requirements (see on page 71 “Considering the power budget requirements”).
- Consider the data link redundancy requirements (see on page 72 “Considering the data link redundancy requirements”).

Refer to the "Installation" user manual, chapters "Technical data > Supply voltage" and "Technical data > Power consumption/power output" for the power requirements of the device.

2.7 Considering the power supply redundancy requirements

[SR7.5]

Check that the power supply redundancy requirements are fulfilled, if required:
- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies themselves are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths as far as possible.

Refer to the "Installation" user manual, chapters "Safety instructions > Requirements for connecting the supply voltage" and "Description > Device views > …" for the power supply redundancy aspects of the device.

2.8 Considering the power budget requirements

Check that the power requirements are fulfilled as required:

- One single power supply can deliver power for every connected device.
  - Also consider the worst-case power requirements of the inserted SFPs.
  - Also consider the inserted media module worst-case power requirements.

Note:
The condition "one single power supply" takes the possible failure of one power supply in a dual power supply configuration into account.

Refer to the "Installation" user manual, chapters "Technical data > Supply voltage" and "Technical data > Power consumption/power output" for the power requirements of the device.

2.9 Considering the data link redundancy requirements

Check that the data link redundancy requirements are fulfilled as required:

- The device has redundant data links (typically for an upstream connection).
- The cabinet or room has redundant data links.
- The redundant data links of the cabinet or the room run along different paths as far as possible.

2.10 Software update

[CR4.3] [NDR3.10] [NDR3.14]

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The following description applies to:
- The initial software update for a device out-of-the-box
- A software update as part of operation or maintenance

Check if an updated release of the device software is available. You find information and software downloads on the Hirschmann product pages on the Internet at catalog.belden.com. Then decide which software release you want to run on your device [NDR 3.10 RE1] <SL-C2>.

2.10.1 Initial access to the device management

To update the software on the device, you need management access to the device.

A device out-of-the-box requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device. After that, HiView allows you to open the Graphical User Interface or the Command Line Interface of the device.

2.10.2 Initial password considerations

In the delivery state, the device has the following user account preconfigured:

Table 17: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
`admin`	`private` (May have been changed at first login.)	`administrator`	The device permits the reading and writing of device management data, including security-relevant settings. The device also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`.
If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 45 “Planning a dedicated user account password policy”).

2.10.3 Software update server considerations

If you want to update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the software files are cryptographically signed.

If you want to perform the initial software update for a device out-of-the-box and you have the new software image on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 86 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the software update server. This enables the device to decide whether the software update server it contacts is trustworthy or not.

Note:
Verify that the server fingerprints are from a trustworthy source, like the server administrator, and that hey have been transferred either in protected form or over a trustworthy network.

2.10.4 Secure boot considerations

Before a possible device software update, determine if you need to apply your secure boot policy, if you have one:

- ☐ Check if the current software and its settings belong to one of the following categories:
  - The image has not been cryptographically signed. Such a software image does not offer the secure boot setting.
  - The image has been cryptographically signed but the secure boot mode is disabled.
- ☐ Check if the new software is cryptographically signed.

If **both** of the above statements are true, apply your secure boot policy (see on page 43 “Planning a secure boot policy <SL-C2>”).

Note:
If you do not have a secure boot policy, to help you decide whether to enable secure boot on that specific device or not, (see on page 48 “Planning configuration encryption and the associated password”)
The secure boot mode is required for a device setup compliant with SL-C2.

If you decide to upload an unsigned software image to the device, verify that the secure boot mode is disabled and that the setting *Allow upload of unsigned device software* is enabled. In the factory setting, the device allows the upload of an unsigned software image ⚠.

Note:
If you enable the secure boot mode, the device no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

If you decide to update the device software:

- ☐ Save the configuration profile in the volatile memory (*RAM*) to the non-volatile memory (*NVM*).
- ☐ Back up the device configuration.
  - If required by your backup policy, save the backup configuration (see on page 57 “Develop a backup policy for device-related data”).
- ☐ Update the device software.
- ☐ Reboot the device for the new software to take effect.

2.10.5 Best practices

To help keep your system secure, consider checking for device software updates regularly and using the latest available release. A newer release of the device software may provide you with security improvements or benefits like new functions, including new device functions that can assist in securing your network.

2.10.6 Detailed documentation

Refer to the "Configuration" user manual,

- Chapter "Managing configuration profiles" for the device configuration profiles
- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts' public key fingerprints.

2.11 Security setup overview

[CR7.1] [CR7.6] [NDR 3.2] [NDR 3.10] [NDR3.14]

The following descriptions apply to:
- The initial device security setup for a device out-of-the-box
- Changes in the device security setup as part of operation or maintenance

Note:
To update the software on the device, you need management access to the device, which requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device.
[CR7.1 RE1] After the IP address setup, HiView offers you to open the device management. For the software update (see on page 73 “Software update”).
[CR3.3] The *Security Status* function in the device GUI can help you gain a first overview of the device security status. The *Security Status* function monitors some security configuration settings that are considered basic. Depending on your requirements, additional security setup steps may be required even if the *Security Status* function reports *ok*.

Refer to:
- The "Graphical User Interface" user manual, chapter "Diagnostics > Status Configuration > Security Status" for the *Security Status* function
- The "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for a basic device security setup

You will find more details for the security setup in the remainder of this chapter.

Note:
To conserve time and effort, you can perform the following security setup steps by loading a prepared configuration profile into the device.
[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 45 “Planning a dedicated user account password policy”).

Note:
If you want to perform the initial security setup for a device out-of-the-box over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.
If you want to perform the initial security setup for a device out-of-the-box and you have the configuration profile on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 86 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the configuration profile server. This enables the device to decide whether the configuration profile server it contacts is trustworthy or not.
Verify that the fingerprints are from a trustworthy source, like the server administrator.

In the following list and the related chapters, "disable logical access" means disabling a feature by a logical measure (a setup in the software). In contrast, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification) (see on page 97 “Possible restrictions to the device’s hardware interfaces”).

Note:
For a device setup compliant with SL-C2, the secure boot mode must be enabled.

The default setting of the secure boot mode is disabled ⚠. If the secure boot mode is disabled, the *Security Status* function in the Web-based interface notifies the user.

If the secure boot mode is enabled but the support mode is also enabled ⚠ (default setting: disabled), the *Security Status* function in the Web-based interface notifies the user.

Note:
If you follow a whitelist approach, consult your necessary function policy. The necessary function policy may stipulate which device functions need to be disabled. This may include functions that are not directly security-related.

Overview of possible security setup steps, in suggested sequence:
- Assign an IP address to the device management:
  - Assign a static IP address (may be considered more secure)
  - Or set up DHCP (depending on your DHCP server policy)
- Disable HiDiscovery access.
- Enable the secure boot mode <SL-C2>.
- Enable configuration encryption <SL-C2>.
- Set up a VLAN dedicated to management access.
- Disable logical access to unused ports and SFP slots.
- Disable logical access for empty media module slots.
- Disable logical access to the signal contact.
- Disable the automatic device software update from the external memory (ACA).
- Disable the SSH key auto upload from the external memory.
- Disable the Configuration load priority for the external memory.
- Disable copying a software file into the device that lacks a valid cryptographic signature.
- Disable writing an unencrypted configuration profile to the external memory (ACA) <SL-C2>.
- Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2>.
- Disable insecure management protocols.
- Enable IP access restrictions.
- Set up a dedicated HTTPS certificate for the device.
- Set up a dedicated SSH host key for the device.
- Set up the SSH Known Hosts fingerprints in the device.
- Set up a dedicated, planned user account login policy.
- Set up a dedicated, planned user account password policy.
- Set up dedicated, planned user account names and roles <SL-C2>.
- Remove user accounts that have standard names <SL-C2>.
- Specify session timeouts <SL-C2>.
- Set up time synchronization for the device clock <SL-C2>.
- Set up logging.
- Disable SNMPv1 traps.
- Enable SNMPv3 traps.
- Set up dedicated login banners.
- Set up the DNS client functions.

You can choose to set up the following advanced device security features as required:
- Access to the system monitor through the serial port
- Disable access to the CLI service shell.

You can also choose to set up the following advanced user authentication measures as required (see on page 95 “Set up advanced user authentication <SL-C2>”):

- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Use MAC authentication bypass for device authentication.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - LDAP
  - RADIUS
  - TACACS+

When the device configuration is complete:

- Create a backup of the configuration according to your backup policy for device-related data.
- If required, include other device-related data like private keys.
- If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and document the HTTPS certificate fingerprint.
- If you plan for accessing the device through SSH and use the self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

2.11.1 Assign IP address parameters to the device management

Note:
At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 45 “Planning a dedicated user account password policy”).

The device offers you the following options for assigning a device management IP address: Local, DHCP (delivery state) ⚠, and BOOTP.

Note:
The setting "Local" (static) is generally considered more secure than using DHCP or BOOTP.
If you use use DHCP or BOOTP, consider loading the configuration or the operating system for the device from the local device memory. This is considered more secure than loading through TFTP. Load from a TFTP server only if you trust the transfer network or if the configuration files are encrypted.

ⓘ Refer to the "Configuration" user manual, chapter "Specifying the IP parameters" on how to specify an IP address for the device management

2.11.2 Disable HiDiscovery access

[CR4.3]

The delivery state of HiDiscovery is enabled ⚠.

Set the HiDiscovery protocol to `Off` after its initial use. This helps make the device more immune against unauthorized discovery and manipulation.

Refer to the "Configuration" user manual, chapter "Specifying the IP parameters using HiDiscovery" on how to:
- Specify the IP address parameters for the device management
- Disable HiDiscovery

2.11.3 Enable the secure boot mode <SL-C2>

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The setting *Secure Boot enabled* disables the booting from a an unsigned software image. This helps secure the device against rogue device software without a valid cryptographic signature.

If you have a secure boot policy, apply your secure boot policy (see on page 43 “Planning a secure boot policy <SL-C2>”) for enabling the secure boot mode on that specific device.

If you do not have a secure boot policy, to help you decide (see on page 43 “Planning a secure boot policy <SL-C2>”).

Note:
The secure boot mode is required for a device setup compliant with SL-C2.

Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Software > Software update" on how to enable the secure boot mode.

2.11.4 Enable configuration encryption <SL-C2>

Enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 48 “Planning configuration encryption and the associated password”).

Note:
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled ⚠. If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.
The configuration encryption password is essentially a symmetric cryptography key, so if you have already planned a policy for symmetric cryptography keys (see on page 37 “Cryptographic key and password basics”), apply it to this key.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/ Save" for the configuration encryption and the associated password.

Options to enable configuration encryption

You have several options to enable configuration encryption:
- If you have a precompiled, unencrypted configuration file:
  - Load the precompiled, unencrypted configuration file.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.

- If you have a precompiled, encrypted configuration file:
  - Enable the configuration encryption and set the associated password manually.
  - Load the precompiled, encrypted configuration file.
- If you do not have a precompiled configuration file:
  - Configure the device manually.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.

2.11.5 Set up a VLAN dedicated to device management access

[SR5.1] [CR5.1] [NDR1.13]

Note:
The prerequisite for working through this section is that you have already performed the planning for the general and security-related device setup (see on page 49 “VLAN plan considerations depending on redundancy protocols”).

The delivery state VLAN ID for device management access is 1.

Set up a VLAN dedicated exclusively to device management access. This helps make the device more immune to potential attacks via the network. It may also help improve the reachability of the device management when there is heavy general network traffic.

Note:
If you use the redundancy protocols *HIPER Ring* or *Ring/Network Coupling*, consider using a VLAN ID ≥2 for device management access. Else, you are free to use any VLAN ID you like.

Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Global > Management interface" on how to specify a VLAN for device management access.

2.11.6 Disable logical access to the signal contact

If you do not need the signal contact, disable the signal contact in the device setup. In the delivery state, the signal contact is enabled in the mode "Monitoring correct operation".

If you do need the signal contact (see on page 99 “Signal contact considerations”).

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status configuration > Signal contact" for the signal contact.

2.11.7 Disable logical access to unused ports and SFP slots

In the delivery state, every port and SFP slot is enabled ⚠.

Disable network access for unused ports and empty SFP slots. Treat inserted SFPs without a data cable connected the same way as an unused port. This helps prevent potential attacks that connect a rogue network device to an unused port.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Port" for disabling ports.

2.11.8 Disable logical access for empty or unused media modules slots

In the delivery state, every media module slot allows access to the network ⚠. With this setting, if a media module is inserted into an empty media module slot, or if ports on an unused media module are physically accessed, the ports of the media module will establish network connections.

Disable empty and unused media module slots in the device setup. This helps prevent potential attacks that connect a rogue network device to a port on a newly inserted or unused media module.

ⓘ Refer to the "Configuration" user manual, chapter "Deactivating the unused modules" for disabling unused media module slots.

2.11.9 Disable the automatic device software update from the external memory (ACA)

The device offers to automatically update the device software during system startup. The prerequisites are:
- The external memory function is enabled.
- On the external memory is a valid software image that is referred to in the file `startup.txt`.

Disable the automatic device software update from the external memory. This helps secure the device against a rogue device software image on an external memory being copied to the device and take effect after a reboot.

In the delivery state setting, the automatic device software update from the external memory is enabled ⚠.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > External Memory" on how to disable the automatic software update from the external memory.

2.11.10 Disable the SSH key auto upload from the external memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:
- The external memory function is enabled.
- On the external memory is a valid SSH key that is referred to in the file `startup.txt`.

Disabling the SSH key auto upload from the external memory can be a reasonable alternative to disabling the external memory function entirely.

Disable the SSH key auto upload from the external memory. This helps secure the device against a rogue SSH key on an external memory being copied to the device and take effect after a reboot.

In the delivery state setting, the SSH key auto upload from the external memory is enabled ⚠.

ⓘ Refer to the "Configuration" user manual:
- Chapter "Basic Settings > External Memory" on how to enable/disable the SSH key auto upload

2.11.11 Disable the Configuration load priority for the external memory

The device offers to assign a priority for the loading of a configuration profile from the external memory:

- *disable*
  The device loads the configuration profile only from the internal non-volatile memory (*NVM*).
- *first*, *second*
  The device loads the configuration profile from the external memory designated as *first*.
  When the device does not find a configuration profile there, it loads the configuration profile from the external memory designated as *second*.
  When the device does not find a configuration profile in the external memory, it loads the configuration profile from the internal non-volatile memory (*NVM*).

In the delivery state setting, the Configuration load priority for all external memories is *first* or *second* ⚠.

ⓘ Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to set the Configuration load priority for the external memory.

2.11.12 Disable copying a software file into the device that lacks a valid cryptographic signature

[NDR 3.2]

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

Disable copying a software file into the device that lacks a valid cryptographic signature: This helps secure the device against rogue device software without a valid cryptographic signature.

If the secure boot mode setting *Secure Boot enabled* is disabled, the device offers you the setting *Allow upload of unsigned device software*. This setting controls whether the device allows the upload of an unsigned software image into the device. If you activate *Secure Boot enabled*, the devide no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

The default setting *Allow upload of unsigned device software* is enabled ⚠. The device will allow the upload a software file into the device that lacks a valid cryptographic signature.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Software > Allow upload of unsigned device software" on how to allow the upload of unsigned device software.

2.11.13 Disable writing an unencrypted configuration profile to the external memory (ACA)

To disable writing an unencrypted configuration file to any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 79 “Enable configuration encryption <SL-C2>”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Load/ Save > Configuration encryption" on how to disable writing an unencrypted configuration profile to the external memory.

2.11.14 Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2>

[CR3.4 RE1]

To disable loading an unencrypted configuration file from any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 79 “Enable configuration encryption <SL-C2>”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Load/ Save > Configuration encryption" on how to disable loading an unencrypted configuration profile from the external memory.

2.11.15 Disable insecure management protocols

[CR4.3] [NDR1.13]

Disable insecure management protocols:
- ☐ Disable SNMPv1/v2 (delivery state: disabled).
- ☐ Disable Telnet (delivery state: disabled).
- ☐ Disable HTTP (delivery state: enabled ⚠ – redirects to HTTPS).

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for disabling insecure management protocols.

2.11.16 Set up management IP access restrictions

[CR3.1] [CR7.7] [CR4.3] [NDR1.13]

The device allows restricting the management access to the device to a source IP address range. You specify the address range by giving an IP address and a netmask.

You can set up the management access IP restrictions individually for each protocol or for a group of protocols.

Table 18: Management access protocol overview

Protocol	Recommended setting for operation	Delivery state
HTTP	Disabled	Enabled ⚠ – redirects to HTTPS
HTTPS	Enabled	Enabled
SNMPv1/v2	Disabled	Disabled
SNMPv3	Enabled	Enabled
Telnet	Disabled	Disabled
SSHv2	Enabled	Enabled
OPC UA Server	Disabled	Disabled

Note:

HTTP (delivery state enabled ⚠) may be useful for the initial setup of the device. However, it is considered insecure for operation. To help secure your system, disable HTTP as soon as you no longer need it, at the latest before your system goes live.

Note:
Confirm that at least one of the set-up management access IP restrictions is active. If no restriction is active, this results in unrestricted management access for every enabled protocol.
Also confirm that for every enabled protocol, at least one of the set-up management access IP restrictions is active. Excluding a protocol from every management access IP restrictions while the protocol itself is enabled, results in unrestricted management access for the respective protocol.

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Activating the IP access restriction" for setting up IP access restrictions.

2.11.17 Set up a dedicated HTTPS certificate for the device

[SR3.1] [SR4.1] [SR4.1 RE1] [CR1.8] [CR4.1] [CR4.3]

<SL-C2> [CR 1.9]

In the delivery state, the device contains a self-signed HTTPS certificate ⚠.

You have the option to:
- Replace the existing HTTPS certificate with a new, self-signed HTTPS certificate on the device
  - To help increase security, use the fingerprint algorithm *sha256* (delivery state: *sha256*) for the self-signed HTTPS certificate fingerprint.
  - After generating a new, self-signed HTTPS certificate on the device, write down its fingerprint for later use when you connect with web browser to the device for the first time.
- Load a dedicated, self-signed HTTPS certificate into the device.

  - If you have control over the entropy used for certificate generation, this way of certificate generation is considered more secure.
  - This alternative is also considered more secure because after generating the HTTPS certificate, you have the certificate and its fingerprint available on your external system. This can help you verify the device HTTPS certificate fingerprint when you connect with a web browser to the device for the first time.
- Load a dedicated, CA-signed HTTPS certificate into the device <SL-C2>
  - If you have an established Public Key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed HTTPS certificate on the device helps you solve the problem "Trust On First Use" when you connect a web browser to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

Note:
If you have an established Public Key Infrastructure (PKI), then loading a dedicated HTTPS certificate onto the device is generally considered more secure and also more convenient. <SL-C2>
You can find possible popular certificate generation tools on the Internet, for example, by searching for the keywords "HTTPS certificate generation".
To help increase security when you create a new, self-signed HTTPS certificate on the device, use the HTTPS certificate fingerprint algorithm *sha256* (delivery state: *sha256*).

Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > HTTPS certificate" for an example of setting up your own HTTPS certificate.

2.11.18 Set up a dedicated SSH host key for the device

[CR1.8] [SR3.1] [SR4.1] [SR4.1 RE1] [CR4.1] [CR4.3]

<SL-C2> [CR 1.9]

In the delivery state, the device contains a self-signed SSH host key .

You have the following options:
- Replace the existing SSH host key with a new, self-signed SSH host key by generating a new SSH host key on the device.
  - To help increase security, use the fingerprint algorithm *sha256* (delivery state: *sha256*) for the SSH host key fingerprint.
  - After generating a new SSH host key on the device, write down its fingerprint for later use when you connect an SSH client to the device for the first time.
- Generate a dedicated SSH host key pair on an external system, self-sign the public key and load the key onto the device.
  - If you have control over the entropy used for key generation, this way of key generation is considered more secure.
  - This alternative is also considered more secure because after generating the SSH host keys, you have the keys and their fingerprints available on your external system. This can help you verify the device SSH host key fingerprint when you connect an SSH client to the device for the first time. <SL-C2>
- Generate a dedicated SSH host key pair, sign the public host key with your Certificate Authority (CA) key and load the CA-signed public host key onto the device.
  - If you have an established public key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed SSH host key on the device helps you solve the problem "Trust On First Use" when you connect an SSH client to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

Note:
You can find possible popular key generation and signing tools on the Internet, for example, by searching for the keywords "SSH key generation tool".

Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > Preparing access using SSH > Loading your own key onto the device" for an example of setting up your own SSH key pair.

2.11.19 Set up the SSH Known Hosts fingerprints in the device

If you want to load the device configuration or update the device software from an SFTP or SCP server, set up the SSH known host fingerprints for these servers in the device. Use the fingerprints of the respective configuration profile or software update servers. This enables the device to decide whether the SFTP or SCP server it contacts is trustworthy or not.

Note:
Verify that the fingerprints are from a trustworthy source, like the server administrator.
If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.

Note:
For authentication, logging, and eMail logging servers, trust is managed by another concept, TLS certificates and revocations lists (see on page 55 “Certificate and revocation management for authentication, logging and eMail servers <SL-C2>”).

Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

2.11.20 Set up a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account login policy (see on page 44 “Planning a dedicated user account login policy”).
For quantitative information on how to ensure a secure login policy (see on page 144 “Attack rate mitigation”). For quantitative information on how to help ensure hard-to-break passwords (see on page 131 “Password strength and policy guide”).

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Apply your planned user account login policy. This helps ensure that the device locks out a user after the specified maximum number of failed user logins in a row, requires a password with minimum length, and enforces the specified waiting period after a failed login.

Set up a dedicated user account login policy as required:

- ☐ Login attempts:
  - Specify the maximum number of failed user logins in a row until the device locks the respective user account (delivery state: 0 – no limit ⚠).
- ☐ Minimum password length:
  - Specify the minimum password length (delivery state: 6 ⚠).
- ☐ Login attempts period:
  - Specify the waiting time (Login attempts period in minutes) before the device auto-unlocks a locked user account (delivery state: 0 – no waiting time ⚠).

Note:
Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port have an unlimited number of login attempts. They are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

2.11.21 Set up a dedicated user account password policy

[CR1.7]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account password policy (see on page 45 “Planning a dedicated user account password policy”).
For quantitative information on how to help ensure hard-to-break passwords (see on page 131 “Password strength and policy guide”).

Set up a dedicated user account password policy as required:

- ☐ Minimum required number of uppercase characters (delivery state: 1 ⚠)
- ☐ Minimum required number of lowercase characters (delivery state: 1 ⚠)
- ☐ Minimum required number of digits in a password (delivery state: 1 ⚠)
- ☐ Minimum required number of special characters (delivery state: 1 ⚠)

Note:
The minimum password length belongs to the user account login policy (see on page 86 “Set up a dedicated user account login policy”).
The enforcement of the password policy belongs to the account names and access roles for device management (see on page 88 “Set up dedicated user account names and access roles for device management <SL-C2>”).

In the delivery state, the device has the following user account preconfigured:

Table 19: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
admin	private (May have been changed at first login.)	administrator	The device permits the reading and writing of device management data, including security-relevant settings. The device also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

Note:
The device asks you to change the delivery state password on the first login. Use a password different from the delivery state password.

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

2.11.22 Set up dedicated user account names and access roles for device management <SL-C2>

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

Note:
The prerequisite for working through this section is that you have already planned a dedicated user account name and access role policy (see on page 46 “Planning a dedicated user account name and access role policy for device management”), and that you have planned a dedicated policy for SNMPv3 authentication and encryption types, and for the related SNMPv3 passwords.
The SNMPv3 passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 37 “Cryptographic key and password basics”), apply it to these keys.

In the delivery state, the device has the following user account preconfigured:

Table 20: User credentials for the administrator account in the delivery state

Username	Password	User account role	Privileges
`admin`	`private` (May have been changed at first login.)	`administrator`	Permits reading and writing of device management data, including security-relevant settings. Also permits the reading of the audit trail.

Note:
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`. If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

Note:
SNMPv3 passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 37 “Cryptographic key and password basics”), apply it to these keys.

Set up dedicated user accounts as required:

- ☐ <SL-C2> Create user accounts. For each new user account, perform the following steps:
  - Create a user account with a dedicated name.
    Note that user account names are case-sensitive.
  - Assign the new user account a strong password.
    Avoid standard passwords like "private" or "public", even for accounts with non-descriptive names.
  - Assign the new user account an access role that offers only the least required privileges.
  - Enforce the password policy check for the new user account (in the delivery state, the password policy check is not enforced ⚠).
  - Save the settings temporarily to let the device check the password of the new account against the enforced password policy.
- ☐ For each new user account, set up an SNMPv3 policy if required:
  - To help increase security, set the SNMPv3 authentication type to *`hmacsha`* (considered more secure than the delivery state *`hmacmd5`* ⚠).
  - Set an SNMPv3 authentication password according to your policy.
  - To help increase security, set the SNMPv3 encryption type to *`aesCfb128`* (considered more secure than the delivery state *`des`* ⚠).
  - Set an SNMPv3 encryption password according to your policy.
- ☐ Help secure existing user accounts:
  - Enforce the password policy check for the existing user accounts (in the delivery state, the password policy check is not enforced ⚠).
  - Set up the SNMPv3 settings as described above for a new user account.

  - If you enforce the password policy subsequently for an existing user account, re-enter the password and save the changed settings temporarily to let the device check the password against the policy.
  - If you change user account data for the currently logged-in user, the device will warn you that you will be logged out.
    To avoid this, consider changing user account data only for user accounts other than the currently logged-in one.
    This may need an additional user account with administrator privileges.
- ☐ <SL-C2> Remove user accounts that have standard names:
  - To remove a user account, first log out of the respective user account and log in with an administrator-role account. Then remove the respective user account.
  - The device requires you to have at least 1 administrator-role account.
    To remove the standard administrator-role account "admin", you need another account with the administrator role. If you haven't, create a new administrator-role account first.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

2.11.23 Specify finite session timeouts <SL-C2>

[CR2.6]

Apply your planned sessions timeout policy. This helps ensure that the device terminates the respective session automatically when idle.

Specify finite session timeouts:

- ☐ Graphical User Interface using HTTPS or HTTP ⚠ (delivery state: 160 min. ⚠)
- ☐ For the Command Line Interface through the serial port, SSH, or Telnet ⚠ (delivery state: 160 min. ⚠)

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial port timeout function

2.11.24 Set up time synchronization for the device clock <SL-C2>

[CR2.11 RE1]

The device offers SNTP and PTP.

The time synchronization protocols SNTP and PTP implicitly trust their time source. Set up the network time synchronization protocol according to the requirements from your overarching network time synchronization policy (see on page 53 "Network time synchronization considerations <SL-C2>").

To receive time information from an upstream time-server, the device has the role of a time synchronization client. To redistribute its time information to other devices, the device has the role of a time synchronization server. Thus, the client role is normally required, for example, for synchronizing the device system clock, whereas the requirement of the server role depends on your network time synchronization policy.

Parameters to be set up may include:
- Enable only the client functions for the time synchronization network protocols allowed by the policy.
- Specify only trusted next-hop upstream time-servers.
- Tune the client functions of the chosen network time synchronization protocol on the device.
- Enable the time synchronization server functions of the device only if required.
- Tune the time synchronization server functions of the chosen network time protocol on the device.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

2.11.25 Set up certificates and possible revocation lists for authentication, logging and eMail servers

<SL-C2> [CR 1.9]

If you intend to use TLS-based servers for one of the following functions, set up the server certificates and possible revocation lists in the device:
- Authentication servers
- Logging servers
- eMail logging servers

This enables the device to decide whether a TLS-based server it contacts is trustworthy or not.

Note:
For software update and configuration servers, trust is managed by another concept, SSH Known Host key fingerprints (see on page 51 “Software update and configuration server considerations <SL-C2>”).

Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > LDAP > Configuration" for managing the certificates for the LDAP client function.
- Chapter "Diagnostics > eMail Notification > Global" for managing the certificates for the email submission function.
- Chapter "Diagnostics > Syslog" for managing the certificates for the Syslog over TLS function.

2.11.26 Set up logging

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR1.2] [CR1.8] [CR2.8] [CR2.9] [CR2.10] [CR2.11] [CR2.12] [CR3.1] [CR3.9] [CR6.1] [CR6.2]

Set up logging:
- ☐ [CR2.11 RE1] Consider setting up the device to synchronize its system clock to a trusted source <SL-C2>.
- ☐ Set up the minimum severity level to be logged.
  The setting depends on our functional and security requirements.
- ☐ Set up logging destinations:
  - The required settings depend on our security requirements.
  - For log availability reasons, a remote destination, different from the location of the device, may be preferable. This is typically a Syslog server.
  - For log confidentiality reasons (logs as data in transit), an encrypted logging protocol may be preferable.
  - For log confidentiality reasons (logs as data at rest), an appropriately secured remote destination may be preferable.

Note:
The Syslog client in the device offers unencrypted communication as well as encrypted communication. The delivery state is unencrypted communication ⚠. To help secure your system, use encrypted Syslog, that is, Syslog over TLS <SL-C2>.

Note:
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > Syslog" for the device Syslog function
- Chapter "Time > SNTP > SNTP Client" on how to synchronize the device clock through SNTP
- Chapter "Time > PTP" on how to synchronize the device clock through PTP

2.11.27 Disable SNMPv1/v2 write access

[CR6.2]

Note:
If you cannot or do not want to disable SNMPv1 (delivery state: disabled) or SNMPv2 (delivery state: disabled) for some reason, consider at least disabling SNMPv1/v2 write access.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > Server > SNMP > Configuration".

2.11.28 Disable SNMPv1 traps

[CR6.2]

The device can send SNMPv1 traps. SNMPv1 traps are unencrypted. From a security perspective, this may be considered insecure.

Disable SNMPv1 traps if you do not need them (delivery state: disabled).

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv1 trap send function.

2.11.29 Enable SNMPv3 traps

[CR6.2]

The device can send SNMPv3 traps. SNMPv3 traps can be signed (authenticated) and additionally encrypted. From a security perspective, authenticated and encrypted SNMPv3 traps are preferable over SNMPv1 traps.

Set up authenticated (and possibly also encrypted) SNMPv3 traps if you require them (delivery state: no SNMPv3 traps configured).

Note:
The SNMPv3 trap passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 37 “Cryptographic key and password basics”), apply it to these keys.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv3 trap send function.

2.11.30 Set up dedicated login banners

[CR1.12]

Set up dedicated login banners:
- ☐ Set up the GUI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- ☐ Set up the CLI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- ☐ Set up the CLI (post-) login banner with only the minimal information required.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Pre-login Banner" for setting up the GUI and CLI pre-login banner
- Chapter "Device Security > Management Access > Command Line Interface" for setting up the CLI post-login banner

2.11.31 Set up the DNS client functions

Consider the possibilities to set up the device's DNS client:
- Disable the DNS client if you do not use it (delivery state: disabled).
- Set up the DNS client to use only the local, static, hostname table.
- Set up the DNS client to use only specified, trusted, external DNS servers according to your DNS server policy.

Note:
If you do not use the DNS client, disabling it is typically considered more secure.
Using only the local, static, hostname table for the DNS client can be considered more secure than using an external DNS server.

Refer to the "Graphical User Interface" reference manual, chapter "Advanced > DNS" for the device's DNS functions.

2.11.32 Advanced: Access to the system monitor through the serial port

You can enable the access to the system monitor via the serial port (V.24/RS-232).

Table 21: Serial port by device type

Device type	Connector type	Connector labeling	Function
EAGLE40-03	RJ45 socket	-	Console access to the device management
EAGLE40-07	DB9 socket	CONSOLE	Console access to the device management
	DB9 socket	COM	None (reserved for future use)

Refer to the "Graphical User Interface" reference manual, chapter "Operation diagnosis > Self-test" on how to enable access to the system monitor via V.24/RS-232.

2.11.33 Advanced: disable access to the CLI service shell

You can disable access to the CLI service shell (delivery state: enabled).

Note:
The CLI service shell can be accessed only by users with the administrator access role.

NOTICE
INOPERABLE DEVICE Disabling the CLI service shell may impair service access. A possible use case when the CLI service shell is needed, is on-site staff needing to issue service shell commands as instructed by the manufacturer support. **Disabling the CLI service shell can result in an inadvertently inoperable device. Disabling the CLI service shell is permanent. To re-enable the CLI service shell, you have to send the device to the manufacturer.**

Refer to the "Configuration" user manual, chapter "User Interfaces > Command Line Interface > Service Shell > Deactivate the Service Shell permanently in the device" on how to disable access to the CLI service shell.

2.11.34 Set up advanced user authentication <SL-C2>

[CR1.2]

Set up the following advanced user authentication measures as required:
- Use 802.1X for user authentication [SR2.3] [SR2.3 RE1] [NDR1.13].
- Use a dedicated authentication policy list.
- Use the MAC authentication bypass for device authentication.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - LDAP, preferably using encrypted communication
  - RADIUS (offers obfuscated communication)
  - TACACS+ (offers obfuscated communication)

Note:
The LDAP client in the device offers encrypted communication as well as unencrypted communication (delivery state: unencrypted communication ⚠). To help secure your system, use encrypted LDAP communication.
The RADIUS client in the device exclusively offers obfuscated communication which is considered weaker than encrypted LDAP.
The TACACS+ client in the device exclusively offers obfuscated communication which is considered weaker than encrypted LDAP.

Note:
If you use authentication servers, this requires setup and maintenance of these external servers. The system operator is responsible to plan and implement these steps.

Refer to:
- The "Graphical User Interface" reference manual:
  - Chapter "Network Security > 802.1X" on how to set up 802.1X port security
  - Chapter "Device Security > Authentication List" on how to set up the authentication policy list of the device’s local IAS

- The "Configuration" user manual chapter "Controlling the data traffic > MAC authentication bypass" on how to set up the MAC authentication bypass
- The "Graphical User Interface" reference manual:
  - Chapters "Device Security > Authentication List" and "Device Security > LDAP" on how to set up the LDAP client in the device
  - Chapter "Network Security > RADIUS" on how to set up the RADIUS client in the device
  - Chapter "Network Security > TACACS+" on how to set up the TACACS+ client in the device

2.11.35 Create a backup of the device-related data

[SR7.3] [SR7.3 RE1]

Create a backup of the device-related data according to your backup policy. This minimizes the effort to replace the device if the device becomes inoperable.

☐ [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Consider creating a backup copy of the device configuration profile <SL-C2>.

☐ Keep the backup files separate from the device in a secure location.
  - For example, place the backup files on a file server in a device-specific folder.

☐ If required and useful, include other device-specific data in the same device-specific folder.
  - For example, include device-specific private keys or certificates.
  - If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and document the HTTPS certificate fingerprint.
  - If you plan for accessing the device through SSH and use a self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on how to save the device configuration.

2.12 Possible restrictions to the device’s hardware interfaces

Note:
The prerequisite for working through this section is that you have already performed planning possible restrictions to the device’s hardware interfaces (see on page 43 “Planning restrictions to the device hardware interfaces”).

The following possible modifications to the device hardware apply exclusively to the device hardware interfaces that are reachable from the device surface. The purpose of these measures is to restrict physical access to particular device interfaces while keeping the device closed.

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Note:
In the following list and the related chapters, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification). In contrast, "disable logical access" a feature by a logical measure (a software setup) (see on page 76 “Security setup overview”).

The following descriptions apply to possible hardware modifications in the following cases:
- For a device out-of-the-box before installation
- After initial installation
- As part of operation or maintenance

Perform the following modification steps to restrict access to the device hardware interfaces, like covering or obstructing a slot or a port, as required. Restrict physical access:
- To the SD card slot
- To the USB port
- To network ports or SFP slots
- To empty media module slots
- To the signal contact
- Restrict physical (visual) access to the device LEDs and port LEDs.

2.12.1 Restrict physical access to the SD card slot

If you have high security requirements, and you are sure you will not need the SD card slot after commissioning, consider covering or obstructing the SD card slot.

ⓘ Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the SD card slot.

2.12.2 Restrict physical access to the USB port

If you have high security requirements, and you are sure you will not need the USB port after commissioning, consider covering or obstructing the USB port.

Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the USB port.

2.12.3 Restrict physical access to network ports or SFP slots

If you have high security requirements, and you are sure you will not need certain network ports or SFP slots after commissioning, consider covering or obstructing these network ports and SFP slots.

Refer to the "Installation" user manual, chapter "Description > Ethernet ports" for the network ports and SFP slots.

2.12.4 Restrict physical access to empty media module slots

If you have high security requirements, and you are sure you will not need certain empty media module slots after commissioning, consider covering or obstructing the empty media module slots.

Refer to the "Installation" user manual:
- Chapter "Installation > Installing media modules" for installing a media module into a slot
- Chapter "Disassembly > Removing a media module" for removing a media module from a slot

2.12.5 Restrict physical access to the signal contact

If you do not need the signal contact and have high security requirements, consider covering or obstructing the signal contact terminals.

If you use the signal contact (see on page 99 “Signal contact considerations”).

Refer to the "Installation" user manual:
- Chapter "Description > Management interfaces > Signal contact" for the signal contact location
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions

2.12.6 Restrict physical (visual) access to the device LEDs and port LEDs

If you have high security requirements, consider performing the following steps:
- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the device LEDs and the port LEDs with a removable cover.

Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

2.13 Device installation

The following description applies to:
- The installation of a device in a new system or system zone
- Changes to the device as part of operation or maintenance

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

2.13.1 Checking the security seal

[NDR 3.13]

On the new device, check the security seal, (see on page 127 “Security seal”).

2.13.2 Data connections

If you have high device availability requirements, use redundant data connections, for example, for an upstream connection.

Refer to the "Installation" user manual:
- Chapter "Installation > Installing an SFP transceiver" for the SFP slots
- Chapter "Description > Ethernet ports" for the network ports
- Chapter "Installation > Connecting data cables" on details how to make data connections

2.13.3 Signal contact considerations

If you use the signal contact, consider the following security and safety aspects:
- **To help protect the device**, connect the signal contact only to a circuit that meets the electrical and safety device requirements.
- **To help protect your system**, connect the signal contact only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit controlled by the signal contact does not have any security or safety function.
  - The controlled circuit does not rely on the secure or safe operation of the signal contact.

Refer to the "Installation" user manual for the signal contact:
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

2.14 Operation

The prerequisite for the operation life cycle phase is that you have taken the appropriate physical and logical steps to set up the device, both regarding functionality and security. This essentially reduces the required security steps during the operation phase to the considerations already described in this security manual, the "Installation" and "Configuration" user manuals, and the "Graphical User Interface" and "Command Line Interface" reference manuals.

As a minimal overview, the essential parts of how to operate the device properly are:

- Environmental conditions (see on page 99 “Device installation”)
- Device availability requirements (see on page 69 “Considering the device availability requirements”)
- Data connections (see on page 99 “Data connections”)

For the privileges and responsibilities of the administrative user roles for both the device hardware and software settings, as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 60 “Operation and maintenance policy”).

2.15 Maintenance

For the privileges and responsibilities of the administrative device user roles as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 60 “Operation and maintenance policy”).

2.15.1 Check the security seal (regularly or triggered by an event)

[NDR 3.11]

On the device, check the security seal, (see on page 127 “Security seal”).

2.15.2 Software update

[NDR 3.10]

If required, perform a device software update.

For the security aspects of the software update (see on page 73 “Software update”).

Refer to the "Configuration" user manual, chapter "Loading software updates" for details on how to:

- Determine the currently running software release
- Determine the stored software release
- Load a previous software version, if required
- Check for a newer available software release
- Update the device software

2.15.3 Hardware changes

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Typical application cases include:

- Connecting or removing an external device on an Ethernet port
- Inserting or removing an SFP

- Inserting or removing a media module on a media module slot
- Connecting or removing a power supply

Note:
Depending on your system availability requirements, provide a redundant data upstream connection.
Consider the worst-case power requirements of the inserted SFPs.
Consider the worst-case power requirements of the inserted media modules.
[SR7.5] Connecting an additional power supply to a device with an existing power supply forms a redundant power supply that helps the device availability. Consider the worst-case device power budget for every power supply, in case one of the redundant power supplies becomes inoperable.

Refer to:
- The "Installation" user manual:
  - Chapter "Description > Ethernet ports" for the network ports and SFP slots
  - Chapter "Connecting data cables" on details how to make data connections
  - Chapter "Installation > Installing an SFP transceiver" for installing an SFP
  - Chapter "Disassembly > Removing an SFP transceiver" for removing an SFP
  - Chapter "Installation > Installing media modules" for inserting a media module into an empty media module slot
  - Chapter "Disassembly > Removing a media module" for removing a media module
- The "Configuration" user manual:
  - Chapter "Configuring the ports > Enabling/disabling the port" for enabling or disabling a port
  - Chapter "Assistance in the protection from unauthorized access > Deactivating the unused modules" for enabling or disabling a media module slot

2.15.4 Device hardware replacement

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

[CR7.4]

Perform the following steps:
- According to your backup policy (see on page 57 “Develop a backup policy for device-related data”)
- According to your hardware replacement policy (see on page 57 “Develop a policy for replacing the device hardware”)

Device hardware replacement steps:
- ☐ On the former device, back up the configuration if required and possible.
  - If you have enabled configuration encryption, document the encryption password.
- ☐ Remove the former device from its environment.
- ☐ [NDR 3.11] On the new device, check the security seal, (see on page 127 “Security seal”).
- ☐ On the new device, perform an initial software update (see on page 73 “Software update”).

- ☐ On the new device, set up the device software, for example, by transferring the existing configuration profiles of the former device to the new device (see on page 76 “Security setup overview”).
  - If you have enabled configuration encryption (see on page 79 “Options to enable configuration encryption”).
- ☐ On the new device, restrict the hardware interfaces if required (see on page 97 “Possible restrictions to the device’s hardware interfaces”).
- ☐ Install and connect the new device in its environment.
- ☐ For the former device:
  - If you want the device repaired, follow your hardware repair policy (see on page 103 “Device hardware repair”).
  - If you want to decommission the device, follow your hardware decommissioning policy (see on page 105 “Device decommissioning”).

Refer to:

- The "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on:
  - How to save the former device’s configuration
  - How to load the configuration into the new device
- The "Configuration" user manual, chapter "Loading software updates" for the new device on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- The "Installation" user manual:
  - Chapter "Disassembly > Removing the device" for mechanically removing the former device from its environment
  - Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the new device

2.15.5 Device hardware repair

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Should your device need repair, follow your device hardware repair policy (see on page 57 “Develop a policy for device hardware repair”).

Consider the following steps:

- ☐ Keep a backup copy of the device configuration (see on page 96 “Create a backup of the device-related data”).
  - If you have enabled configuration encryption, document the encryption password.
- ☐ Make a note of the device base MAC address (read it from the label on the front panel or look it up in the device management).
- ☐ If required and possible, wipe or delete the configuration and other data you consider confidential (see on page 105 “Deletion of confidential data and secrets”).
- ☐ Record the condition of the security seal on the device (see on page 127 “Security seal”).

☐ Send the device to the manufacturer for repair.
☐ When the device is back from repair:
  – Check according to your device hardware repair policy if the device you received back is acceptable (is either identical to the device you sent in, is a different device of the same type, or is a different device of a superior type).
  – Check the security seal of the repaired device, (see on page 127 “Security seal”). The security seal on the identical device received back should either be a new security seal or the old security seal shall be approximately in the same condition as when you sent the device in. If the device you received back is a different device of the same type or a different device of a superior type, it should have a new security seal.
  – If you have enabled configuration encryption (see on page 79 “Options to enable configuration encryption”).
  – Restore the files on the repaired device from the backup.
  – If required by your policy, compare the repaired device’s actual base MAC address with the address you noted earlier. This helps ensure you have the same device back that you sent in.
  – If required, update the software on the repaired device.

ⓘ Refer to the "Installation" user manual:
- Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the repaired device

2.16 Device decommissioning

When decommissioning a device, follow your device hardware decommissioning policy (see on page 58 “Develop a policy for device hardware decommissioning”).

⚠ WARNING

ELECTRIC SHOCK

To avoid electric shock, do not open the device.

Failure to follow these instructions can result in death or serious injury.

Note:
If you have high security requirements, consider physical destruction of the device and the external memory (ACA)(see on page 106 “Secure physical destruction of the device and its accessories”). Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping unnecessary (see on page 105 “Deletion of confidential data and secrets”).
If you plan to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

ⓘ Refer to the "Installation" user manual, Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment.

2.16.1 Deletion of confidential data and secrets

Note:
Resetting the device to the delivery state performs normal file deletion operations on the device, and on the external memory (ACA), which may leave parts of the file contents or memory blocks in the flash memory intact [CR4.2]. Furthermore, the audit trail persists after a reset to the delivery state.
If you have high security requirements, consider the physical destruction of the device and the external memory.

2.16.2 Reset to the delivery state

For the deletion of data, perform the following steps as required:

- Reset the device to the delivery state. This performs the following operations:
  - Deletes the configuration profiles and configuration scripts in the device.
  - If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.
  - Resets the boot parameters.
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.

  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - If the external memory (ACA) is plugged in, the device also deletes the configuration profiles on the external memory.
- If required, manually delete other files on the external memory.

Note:
The audit trail persists in the device even after a reset to the delivery state.

Refer to the "Configuration" user manual, chapter "Managing configuration profiles > Reset the device to the factory defaults" on how to reset the device to the delivery state.

2.16.3 Secure physical destruction of the device and its accessories

For the secure physical destruction of physical components, perform the following steps as required by your decommissioning policy:

- ☐ Destroy the security seal on the device, (see on page 127 “Security seal”).
- ☐ Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device
  - The SSH host key pair in the device
  - The configuration profiles in the device
  - Any other files in the device
- ☐ If required, physically destroy the external memory (ACA). This addresses:
  - The configuration profiles on the external memory
  - The software files on the external memory
  - Any other files on the external memory

2.16.4 Secure removal of device-related data from the administration environment

<SL-C2> [CR 1.9]

For the secure removal of device-related data from the administration environment, perform the following steps as required by your decommissioning policy.This may include:

- ☐ The removal of configuration data and its backups
- ☐ The removal of private cryptographic keys
- ☐ The removal of self-signed certificates
- ☐ The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

2.16.5 Secure disposal of the device hardware

For the secure disposal of the device hardware, follow your disposal policy.

Note:
If you have high security requirements, consider disposing of the device by shredding it.

3 Network security support

This main chapter describes how the device can assist in:
- Securing your system
- Improving the availability of your system

This chapter deals with specific device functionality in the operation and maintenance life cycle phases that can help improve the security or availability of your network.

3.1 Introduction

Aside from the basic task of forwarding and processing data packets in your network, the device can also help:
- Deploy defense in depth for your network
- Harden your network
- Enhance and maintain the availability of your network

3.1.1 Prerequisites for setting up network security

Only a device that is itself already secured can help reasonably improve the security and availability of your network. The prerequisite for working through this section is that you have taken the required steps to securing the device itself (see on page 63 “Device security in the life cycle phases”).

To determine which device functions are suitable for providing or enhancing the security of your network, apply the process of assessing threat risks, mitigation efficiency and the criticality of the individual threat risk/mitigation efficiency combinations analogous to the device-centered process:
- Compile a network threat profile (see on page 26 “Compiling a threat profile”):
  - Develop a network threat model.
  - Collect the perceivable threats to the network.
  - Assess the network threat risks.
- Develop a general network defense strategy (see on page 28 “Defense in depth vs. hardening”).
- Develop a general network mitigation strategy (see on page 31 “Developing a mitigation strategy”):
  - Collect the perceivable network mitigations.
  - Assess the network mitigation efficiency.
- Develop an individual mitigation strategy (see on page 34 “Criticality assessment and mitigation strategies”):
  - Assess the criticality of the individual network threat/mitigation combinations.
  - Develop a mitigation strategy based on the individual criticality values.

3.1.2 Deploying defense in depth for your network

Defense in depth creates several barriers that a potential attacker must overcome one after the other. The prerequisite for working through this section is that you have already set up a dedicated plan for defending your network in depth (see on page 28 “Defense in depth”).

From a system view, there are 2 complementary ways to implement defense in depth for a network:

- The device-related way:
  The device-related way deploys measures to help secure the device itself. This in turn helps secure the network. These measures are described in the preceding main chapter (see on page 76 “Security setup overview”).
- The network-related way:
  The network-related way deploys specific device functions as measures to help secure the network. These measures are described in the remainder of this main chapter.

The suggested network-related mitigation measures are collected in the following chapter (see on page 109 “Measures to help secure the network”).

Note:
First pick the mitigation measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

3.1.3 Harden your network

The suggested network-related mitigation measures are collected in the following chapter (see on page 109 “Measures to help secure the network”).

Note:
Pick the mitigation measures suitable for defense in depth first. Then pick hardening measures from the remaining options.

3.2 Measures to help secure the network

The below collection of network-related mitigation measures can be used for defense in depth as well as for hardening. First pick the measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

To help you secure your network, perform the following steps on the device according to your requirements, threat and mitigation assessment results, and policies:

- Restrict logical access to your network:
  - Set up VLANs for traffic segregation.
  - Disable GVRP and MVRP.
  - Set up Port Security.
  - Set up *DHCP Snooping*
  - Set up *IP Source Guard*
  - Set up *Dynamic ARP Inspection*
  - Set up the MAC authentication bypass.
- Help secure the network protocols used.
  - Disable GMRP and MMRP.
- Help secure the redundancy protocols used:
  - Set up RSTP guards and helper protocols.
  - Set up the *MRP* (MRP VLAN ID ≥2, tagged packets) parameters.
  - Set up MRP over LAG (MRP VLAN ID ≥2, tagged packets)]
  - Set up Sub Ring with LAG (MRP VLAN ID ≥2, tagged packets)
  - Set up the *HIPER Ring* parameters.
  - Set up HIPER Ring over LAG (VLAN ID 1: tagged packets)
  - Set up the *Redundant Coupling Protocol* parameters.
  - Set up *Ring/Network Coupling* parameters.
- Set up the attack protection support functions:
  - Set up the Denial of Service (DoS) parameters.
  - Set up the Access Control Lists (ACLs).
  - Set up the rate limiter.
  - Set up the Management MAC address conflict detection
- Set up the network time synchronization parameters.
- Set up the logging parameters.
- Set up the LLDP parameters.

Note:
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.
Routing protocols like HiVRRP, VRRP, OSPF or RIP are outside the scope of this document.

3.3 Restrict logical access to your network

3.3.1 Set up VLANs for traffic segregation

[SR5.1] [CR5.1]

The essential prerequisite for setting up VLANs in the device is that you have created a VLAN plan for your network (see on page 39 “VLAN plan”).

Set up the VLANs, the port memberships and the properties of the port memberships according to your VLAN plan.

Note:
If you use certain redundancy protocols, consider using only VLAN IDs ≥2 for payload traffic and device management (see on page 49 “VLAN plan considerations depending on redundancy protocols”).

Refer to the "Graphical User Interface" reference manual, chapter "Switching > VLAN" on how to set up VLANs for traffic segregation.

3.3.2 Disable GVRP and MVRP

The GARP VLAN Registration Protocol (GVRP) and its successor, the Multiple VLAN Registration Protocol (MVRP or MRP-IEEE Multiple VLAN Registration Protocol) can be used to dynamically set up VLANs in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GVRP or MVRP frames or inject deliberately crafted GVRP or MVRP frames.

It is generally considered more secure to disable GVRP and MVRP.

Note:
The delivery state for both GVRP and MVRP is globally disabled.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > GARP > GVRP" on how to set up GVRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple VLAN Registration Protocol" on how to set up MVRP

3.3.3 Set up the Port Security

[NDR 1.13]

Port Security is a concept to restrict which frames the network device accepts that have been received on a specific port or VLAN. This can help secure your network.

Port Security distinguishes frames by their MAC source address and their VLAN tag. These values identify frames sent by another device in the L2 network. The device drops frames with a disallowed MAC source address or VLAN ID.

To set up Port Security, create a list of allowed MAC source addresses and VLAN IDs. If the device receives a frame with a MAC source address that is not on the allow list, the device can take a configurable action like sending an SNMP trap to the network management station or disabling the port.

Note:
The delivery state for the Port Security operation is globally disabled. The sub-function "Auto-disable" is also disabled.
Activating Port Security can help protect your network against injection of frames from unknown network nodes. However, if the Port security function is configured to auto-disable a given port when the function detects undesired frames, this can lead to a Denial of Service (DoS) situation. An attacker may even deliberately send deliberately crafted frames to cause a DoS.
Configure the Port Security function according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > Port Security" on how to set up Port Security.

3.3.4 Set up DHCP Snooping

DHCP Snooping is a function that supports the network security. It monitors DHCP packets between the DHCP clients and the DHCP server and acts like a specialized firewall between the untrusted DHCP clients and the trusted DHCP servers. *DHCP Snooping* supports you in protecting the network against attacks through rogue or mis-configured devices on untrusted ports or in untrusted VLANs, by filtering or rate-limiting DHCP client packets.

Note:
The delivery state for the *DHCP Snooping* sub-functions "Verify MAC" and "Auto-disable" is disabled.
Activating *DHCP Snooping* can help protect your network against rogue network nodes requesting a legitimate IP address. However, if the*DHCP Snooping* function is configured to auto-disable a given port when the function detects a rogue node, this can lead to a Denial of Service (DoS) situation. An attacker may even deliberately send deliberately crafted frames to cause a DoS.
Configure the *DHCP Snooping* function according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > DHCP Snooping" on how to set up DHCP Snooping.

3.3.5 Set up IP Source Guard

IP Source Guard is a function that supports the network security. It filters IP data packets received from another device (called the subscriber), based on the source ID (source IP address or source MAC address). *IP Source Guard* supports you in protecting the network against attacks through IP/MAC address spoofing.

IP Source Guard relies on the *DHCP Snooping* function (see on page 111 “Set up DHCP Snooping”) for determining trusted source IDs, VLANs, and ports for known subscribers, so you have to set up the *DHCP Snooping* function before you can use the *IP Source Guard* function.

IP Source Guard uses the *Port Security* function (see on page 110 “Set up the Port Security”) for controlling the actual data packets, so you have to also set up the *Port Security* function before you can use the *IP Source Guard* function.

Note:
Activating the *IP Source Guard* function can help protect your network against rogue network nodes requesting a legitimate IP address. However, if the *DHCP Snooping* function or the Port security is configured to auto-disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS.
Configure the *IP Source Guard* function according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > IP Source Guard" on how to set up IP Source Guard.

3.3.6 Set up Dynamic ARP Inspection

Dynamic ARP Inspection is a function that supports the network security. This function analyzes ARP packets originating from an untrusted port or destined to an untrusted port, and can rate-limit ARP packets as well as log and discard invalid ARP packets.

Note:
The delivery state for the *Dynamic ARP Inspection* sub-functions "Verify source MAC", "Verify destination MAC", "Verify IP address", and "Auto-disable" is disabled.
Activating *Dynamic ARP Inspection* can help protect your network against rogue network nodes trying to diverting and snoop or manipulate legitimate traffic. However, if the *Dynamic ARP Inspection* function is configured to auto-disable a given port when the function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS.
Configure the *Dynamic ARP Inspection* function according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > Dynamic ARP Inspection" on how to set up Dynamic ARP Inspection.

3.3.7 Set up the MAC authentication bypass

If required, set up the MAC authentication bypass for device authentication.

The MAC authentication bypass can authenticate a particular user of another device, for example the laptop of maintenance personnel, without the need to set up the Port Security of the local network device to allow the MAC source address of the other device.

The advantages are:

- The MAC source addresses of the allowed external devices need not be locally set up in the network device.
- You are spared the local administration effort if the MAC source address changes (for example, because a maintenance laptop has been replaced).
- The external device is not restricted to authentication on a specific network device port.

Note:
The MAC authentication bypass function requires an external authentication server.
If you have high security requirements, disabling the MAC authentication bypass and instead temporarily setting up the maintenance laptop’s MAC address locally on the device may be considered more secure.

Refer to:

- The "Configuration" user manual, chapter "Controlling the data traffic > MAC authentication bypass" on how to set up the MAC authentication bypass
- The "Graphical User Interface" reference manual, chapter "Network Security > 802.1X > 802.1X Global > MAC authentication bypass format options" on the MAC authentication bypass format

3.4 Help secure the network protocols used

3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) and its successor, the Multiple MAC Registration Protocol (MMRP or MRP-IEEE Multiple MAC Registration Protocol), can be used to register group (that is, Multicast) MAC addresses dynamically and to automatically setup Multicast forwarding in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GMRP or MMRP frames or inject deliberately crafted GMRP or MMRP frames.

It is generally considered more secure to disable GMRP and MMRP.

Note:
The delivery state for both GMRP and MMRP is globally disabled.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > GARP > GMRP" on how to set up GMRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple MAC Registration Protocol" on how to set up MMRP

3.5 Help secure the redundancy protocols used

Note:
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.

3.5.1 Set up RSTP guards and helper protocols

[CR3.1]

If you use RSTP, consider securing the RSTP guards:
- Consider enabling the BPDU guard function on Edge ports (delivery state: disabled).
- Consider enabling the BPDU filter function on Admin Edge ports (delivery state: disabled).
- Consider disabling the BPDU flood function on ports that have RSTP disabled (delivery state: disabled).

Help secure RSTP helper protocols:
- Consider disabling the L2 loop protection (delivery state: disabled). This helps protecting against a possible DoS attack, where an attacker sends malicious loop protection frames to the device, intending to trick it into disabling its respective port.

Note:
Enabling RSTP guards and helper protocols can help protect your network against rogue network nodes trying to diverting, snoop or manipulate legitimate traffic. However, if a function is configured to auto-disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS. Configure the RSTP guards and helper protocols according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Global" on how to set up the BPDU guard and BPDU filter in the device
- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Port" on how to set up the Root guard, TCN guard, the port-related BPDU filter and the BPDU flood functions
- Chapter "Diagnostics > Loop Protection" on the device L2 loop protection function.

3.5.2 Set up the MRP (Media Redundancy Protocol) parameters.

[SR5.1] [CR5.1] [CR3.1]

If you use MRP, consider:
- Using tagged packets for the MRP VLAN
  This helps MRP availability by prioritizing MRP control packets.
- Specifying a MRP VLAN ID ≥1
  This causes MRP to use a standard VLAN tag in MRP control packets. This may require an existing VLAN plan.

Note:
The delivery state for MRP is disabled in the device, the MRP VLAN ID is 0.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > MRP" on how to set up MRP.

3.5.3 Set Up MRP over LAG

Set Up MRP over LAG (MRP VLAN ID ≥1, tagged packets). This may require an existing VLAN plan.

Note:
The delivery state for MRP is disabled in the device, the MRP VLAN ID is 0.

Refer to the "Configuration" user manual, chapter "Redundancy > Media Redundancy Protocol (MRP) > MRP over LAG" on how to set up MRP over LAG.

3.5.4 Set up Sub Ring with LAG

Set up the Sub Ring with LAG function with an MRP VLAN ID ≥2 and tagged packets. This may require an existing VLAN plan.

Note:
The delivery state for the Sub Ring is disabled in the device, the MRP VLAN ID is 0.

Refer to the "Graphical User Interface" reference manual, chapter "Redundancy > Sub Ring with LAG" on how to set up Sub Ring with LAG.

3.5.5 Set up the HIPER Ring parameters

[SR5.1] [CR5.1] [CR3.1]

If you use the *HIPER Ring* function, consider setting up tagged packets for the fixed VLAN ID 1. This helps the availability of the *HIPER Ring* by prioritizing *HIPER Ring* control packets.

This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *HIPER Ring* is globally disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *HIPER Ring*" on the device *HIPER Ring* function.

3.5.6 Set Up HIPER Ring over LAG

Set Up HIPER Ring over LAG with the fixed VLAN ID 1 and tagged packets. This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *HIPER Ring* is globally disabled.

Refer to the "Configuration" user manual, chapter "Redundancy > HIPER Ring client > HIPER Ring over LAG" on how to set up HIPER Ring over LAG.

3.5.7 Set up the Redundant Coupling Protocol parameters

[CR3.1]

If you use the *Redundant Coupling Protocol*, consider helping secure the *Redundant Coupling Protocol*, for example, by setting up VLANs according to your VLAN plan.

Note:
The delivery state for the *Redundant Coupling Protocol* is globally disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *Redundant Coupling Protocol*" on the device *Redundant Coupling Protocol*.

3.5.8 Set up Ring/Network Coupling parameters

[SR5.1] [CR5.1] [CR3.1]

If you use *Ring/Network Coupling*, consider setting up tagged packets for the fixed VLAN ID 1 (delivery state: untagged). This helps harden the *Ring/Network Coupling* by prioritizing *Ring/Network Coupling* control packets.

This may require an existing VLAN plan with a device management VLAN ID ≥2.

Note:
The delivery state for the *Ring/Network Coupling* is globally disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > *Ring/Network Coupling*" on the device *Ring/Network Coupling* function.

3.6 Set up the attack protection support functions

3.6.1 Set up the Denial of Service (DoS) parameters

[CR7.2]

Consider setting up DoS filters.

Note:
The delivery state for the DoS filters is globally disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > DoS > DoS Global" on the device DoS filter functions.

3.6.2 Set up the rate limiter

[CR7.2]

Consider setting up the rate limiter for broadcast, Multicast or Unknown Unicast frames.

Note:
The delivery state for the broadcast, Multicast or Unknown Unicast rate limiters is disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > Rate Limiter" on the device Rate Limiter functions.

3.6.3 Set up the Management MAC address conflict detection

[NDR1.13]

Consider activating the Management MAC address conflict detection for the device management address. If the function is active and the device detects a conflict, the device will send a trap.

Note:
The delivery state for the Management MAC address conflict detection is disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Network > Global > Management interface" on the device’s Management MAC address conflict detection function.

3.7 Set up Access Control Lists (ACLs)

[CR7.2] [NDR 1.13] [NDR5.2] [NDR5.2 RE1] [NDR5.3]

This chapter deals with ACLs, their function and the suggested setup steps. It describes the basic ACL functions. Extended ACL functions are outside the scope of this chapter.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > ACL" for the device ACL function.

3.7.1 Introduction

Access Control lists (ACLs) offer extensive and fine-grained control over the forwarding or dropping of data packets received or transmitted by the device. ACLs can therefore be useful to mitigate security threats in a straightforward yet detailed way.

Note:
In the GUI, an ACL is referred to as a "Group" (a rule group) that has a name and contains one or more rules.

A rule consists of:
- One or more criteria that have to match simultaneously (like a device port number, or an L3 protocol field) and
- One or more actions (mainly `permit` or `deny`) that the device takes when a data packet matches the rule's criterion

The following rule features are outside the scope of this chapter:
- A rule can have the following extended criteria:
  - The operators `not equal to`, `less than`, and *greater than* for Layer 4 port numbers (source or destination).
  - The operator `fragmented IPv4 packets`
  - The operator `IGMP type`
  - The operator `ICMP type and code`
  - Operators for the TCP flags `ACK`, `RST`, `FIN`, `PSH`, `SYN`, `URG`, and established (`ACK` or `RST`)
- A rule can have the following actions:
  - Creating a log entry
  - Limiting the data rate
- A rule can have the following extended actions:
  - Redirection to a specific port
  - Mirroring to a specific port
  - Assigning a specific queue ID
- A rule can be time-based. That is, the device activates or deactivates a time-based rule, based on the device system time. A time range can be an absolute or periodic time and date. A time range is identified by a name that is referenced in the ACL rule.

Each rule belongs to an ACL with a specific name and has the same type (IPv4-based) as the ACL and its sibling rules. Rules belonging to the same ACL are processed in ascending order of the individual rule index.

Every ACL has an implicit, invisible `deny` rule as the last rule <SL-C2>. As a result, if no explicit rule of an ACL matches a data packet, the device drops the data packet.

Note:
The IPv4-based numerical range starts with 1000.

For an ACL to take effect, assign the ACL: Choose a device port (source or destination port) or a VLAN. Assign a priority to this association, choose the desired direction of the data flow the ACL association shall apply to, and finally select an existing ACL name (followed by the ACL's internal number).

Properties of ACL assignments:
- On a device, 2 or more ACLs can be active simultaneously.
- Each assignment has a priority.
- If there are 2 or more ACLs of the same type assigned to the same device port or VLAN, the device processes the ACL with the higher priority first.
- If the same ACL is assigned to both a port and a VLAN, the device processes the port-related assignment first.
- A particular ACL can be assigned to more than one device port or VLAN, for example, to allow for bidirectional packet flow.

Note:
The device can apply ACLs only to received data packets.

Note:
To help ensure a defined processing order, specify for each assignment a priority that is unique in the scope of the device.

Because ACLs have a potentially heavy impact on the forwarding of data packets, ACLs should be planned accurately and generally need to be tested. If possible, test your planned and set-up ACLs in a test environment before applying the ACLs in a production environment. This allows for the modification, addition, or deletion of rules, ACLs, or ACL assignments that may have been overlooked during planning.

3.7.2 Resolving potential conflicts of aims for an ACL

When creating or modifying an ACL, there can be a conflict of aims between the security aspects of the network and the desire for the smooth functioning of the network:
- Security aspects of the network require the ACLs to be as restrictive as possible and to set up only the smallest possible set of `permit` rules. These ACLs are preferably applied to incoming data packets to drop unwanted data packets at the earliest possibility, and also to minimize the traffic within the device.
- Smooth functioning of the network desires the ACLs to be as permissive as possible and to set up only the smallest possible set of `deny` rules. The ACLs can be applied to outgoing data packets to maximize possible data packet processing in the device and to drop only the explicitly undesired data packets.

One possible way to address this conflict of aims is to put security first. That is, you plan and set up only the explicitly required `permit` rules. If the test results indicate that ACLs or their assignments are too restrictive, you can modify the ACLs (for example, add new `permit` rules) or their assignments appropriately.

3.7.3 Creating ACLs and associations

The following section describes one possible way of planning, setting up, testing, and administering ACLs for a device. Adapt these steps to suit your specific situation. Some steps may need to be applied iteratively.

Note:
You can plan the ACLs by setting up the ACLs directly on the device, or by using an off-line process and uploading the resulting ACLs to the device later.

Planning

- ☐ Make a list of packet types that explicitly need to be forwarded by the device.
- ☐ Common criteria for packets are (not exhaustive):
  - For an IPv4-based ACL: Source IP address, destination IP address, protocol, source TCP/UDP port, and destination TCP/UDP port
- ☐ As data traffic is typically bidirectional, plan 2 ACLs to consider the data packets for both directions. If the ACLs for different data directions are identical, consider creating only one ACL and assign it separately to each data direction, if possible.
- ☐ Determine to which device port or VLAN you assign the planned ACLs.
- ☐ Consider if it is advantageous to split up the set of packet types into subsets, so each subset can be processed by a particular ACL of a given type, assignment, and data packet direction. Name the individual ACLs (groups) to reflect the ACL's purpose, and, for example, by using a common name prefix for related ACLs.
- ☐ For each ACL, order its rules, using the following criteria:
  - Put the `permit` rule with the most general criteria first (for example, every packet with a certain VLAN tag). Give this rule the lowest index within the ACL. This takes care of the ACL function aspect.
    In the simplest case, this rule is general and has no exceptions. If exceptions are required, deal with them in the next planning step, "Refine the rule list…".
  - Put the `permit` rule with the second-most general criteria next (after the previous rule) by giving it a higher index than the first rule.
  - Proceed with the remaining `permit` rules in this order.
- ☐ Refine the ACL by planning exceptions:
  - For required exceptions to an `permit` rule, put a specific `deny` rule before the respective `permit` rule by giving it a lower index than the existing `permit` rule. This takes care of the ACL security aspect.
  - If further exceptions are required, insert the respective new `deny` rules before the respective existing `permit` rule (give it a lower index). This takes care of the ACL security aspect.
  - Put the rule with the most general exception first (give it the lowest index), followed by the rule with the second-most general exception (give it the second-lowest index), and so on.
  - Repeat these steps for every required exception in the given ACL.
  - A new `deny` rule may turn out to be too general and may therefore require further exceptions in the form of one or more additional preceding `permit` rules. This takes care of the ACL function aspect.

Note:
ACLs and their assignments can become complex. Consider testing the ACLs before you deploy them.

Setup

- ☐ Use the GUI, CLI, or network management software to set up the planned ACLs on the device, or
- ☐ Upload a configuration script (for example, generated by an offline configuration tool) to the device.

Test

- ☐ Activate and assign the ACLs on the device in a test setup.
- ☐ Generate test traffic that represents the expected traffic, that is, consisting of desired as well as of undesired data packets.
- ☐ Evaluate the packets received on the test end devices:
  - Look for unexpected packets. If unexpected undesired packets are transmitted by the test device, add a matching `deny` rule to the ACL plan and subsequently to the respective ACL. Note that the unexpected, undesired packets may include packets targeted at the device-under-test's management.
  - Look for missing packets. If expected desired packets are not received on the test end devices, consider adding a matching `permit` rule to the ACL plan and subsequently to the respective ACL.
    Note that the expected desired packets may include packets sent by the device-under-test's management.
- ☐ Evaluate the log entries created by the device:
  If you have configured your ACL rules to create log entries, inspect the log entries. This can be useful to determine, for example, why the device has dropped a packet.

Administration

- Give the ACLs descriptive names, for example, showing their purpose, possibly including the assignment to a port or VLAN, and the data direction.
- Consider:
  - Saving the ACLs separately from the device configuration or in addition to the device configuration, for example, as script files
  - Assigning the ACL a version number, if you have separate script files for each ACL
  - Using version control to track the ACL history

3.8 Set up the network time synchronization parameters <SL-C2>

[CR2.11 RE1]

The prerequisite for working through this section is that you have taken the required steps to help secure the device itself (see on page 90 “Set up time synchronization for the device clock <SL-C2>”).

To synchronize its system clock, the device acts as a network time client. To help synchronize the time in the network, the device can also act as a network time-server.

Set up the time functions of the device:
- Enable the client function of the device, if required.
  - Enable only the client functions for the network time protocol allowed by your policy.
  - Tune the client functions of the chosen network time protocol on the device.
- Enable the server function of the device only if required.
  - Enable only the server functions for the network time protocol allowed by your policy.
  - Tune the server functions of the chosen network time protocol on the device.

Note:
The delivery state for the time functions is globally disabled.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Time > SNTP" for the device SNTP client and server functions
- Chapter "Time > PTP" for the device PTP functions

3.9 Set up the logging parameters

[CR1.2] [CR1.8] [CR2.11] [CR3.1]

Set up logging severity levels and destinations. The required settings depend:
- on your device logging policy
- on your remote logging policy

Note:
In the delivery state, the Syslog function is globally disabled.
The Syslog client in the device offers unencrypted communication as well as encrypted communication (that is, Syslog over TLS). The delivery state is unencrypted communication ⚠.
To help secure your system, use encrypted Syslog <SL-C2>.
[CR2.11 RE1] Secure logging also relies on the synchronization of the device system clock to a trustworthy source (see on page 90 “Set up time synchronization for the device clock <SL-C2>”).
The persistent logging function, which writes logged events to a device-internal log, can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once created and written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device Syslog function.

3.9.1 Audit trail (created by persistent logging)

[CR2.11]

The persistent logging function itself can be enabled or disabled. However, existing audit trail entries persist even after the persistent logging function has been disabled.

Note:
The audit trail cannot be deleted by resetting the device to the delivery state.

3.10 Set up the LLDP parameters <SL-C2>

The LLDP global operation setting can be *On* or *Off*. The delivery state is *Off* (disabled).

The device also offers the following basic port-related LLDP operating modes:

- *transmit*
  - The port transmits information about the device and the port itself to its neighbors.
  - The neighbors can collect that information, provide it to a management station, or process it themselves. The prerequisite is that the other devices in the same network have their individual *receive* function enabled.
- *receive*
  - The device collects information about its neighbors that it receives at the given port.
  - The device can provide this information to a management station or process the information itself. The prerequisite is that the other devices in the same network have their individual *transmit* function enabled.
- *receive and transmit* (delivery state ⚠)
  - The port transmits information about the device and the port itself to its neighbors.
  - The device also collects information about its neighbors that it receives at the given port.
- *disabled*
  - The port neither transmits any information about the device or the port itself, nor does it collect information received from other devices.

Enabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Drawback: The device sends information about itself to its immediate neighbors. This might pose an attack surface.
  - Drawback: LLDP-unaware neighbors (for example, a hub) may distribute the device information beyond the immediate neighbors, possibly to the entire L2 network, which might pose an additional attack surface.
  - Advantage: The device can indirectly detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor and report that event to a management station.
- Functional aspects:
  - Advantage: Topology discovery: The device can help perform a system inventory by collecting information about its neighbors and providing this information to a management station.
  - Advantage: The device can use the received information, for example, to automatically detect a duplex mismatch between one of its ports and the given port's immediate neighbor without the need to set up the Port Monitor function.

Disabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Advantage: The device does not send out any explicit information about itself. This reduces the attack surface.
  - Drawback: The device cannot detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor.
- Functional aspects:
  - Drawback: No Topology discovery: The device cannot help perform a system inventory.
  - Drawback: The device cannot automatically detect, for example, a duplex mismatch. For that, the Port Monitor function needs to be set up.

The above lists are not exhaustive. Evaluate the possible LLDP settings on the device according to your planned LLDP policy.

Enable or disable LLDP globally and choose the port-related operation modes according to your planned LLDP policy. You may elect to enable only the receive function. Setting up LLDP on the device may require that other network devices have their own LLDP function appropriately enabled.

Refer to:

- The "Graphical User Interface" reference manual, chapter "Diagnostics > LLDP > LLDP Configuration" for the device LLDP function
- The "Configuration" user manual, chapter "Operation diagnosis > Topology discovery" for an explanation of LLDP use cases

A Security seal

A.1 Overview

<SL-C2> [NDR 3.11]

The devices are equipped with mechanical components that have the function of a security seal. The type and location of the security seal depends on the device hardware family.

The purpose of the security seal is:
- To either thwart attempts to manipulate the internal hardware of the device
- Or to uncover manipulations through visible traces

A security seal can be of the following type:
- Glued front label (see on page 128 “Glued front label”)
- Potted device (see on page 129 “Potted device”)
- Security stickers (see on page 129 “Security stickers”)

A.2 Details

The following chapters describe the properties and procedures for the mechanical security components, also called security seals.

Note:
The decommissioning procedures describe only the minimum steps to mark the security seals as decommissioned. Depending on your situation, additional decommissioning steps may be required.

A.2.1 Glued front label

Security properties:
- The front label is glued to the front panel and completely covers the screws that are needed to open the device.
- There are no other screws that permit opening the device.

Tampering evidence:
- The front panel has exposed screws.
- The front label has cutaways, cuts, scratches, wrinkles or folds, especially in the corners where the screws are located.

Check procedures:
- New device:
  - Check that the front label is new and has no exposed screws, cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the front label.
    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
- Repaired device back from manufacturer:
  - If the device and the front label are both the same:
    Check the condition of the front panel against the recorded condition. The front label shall be approximately in the same condition as before.
    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device is the same but the front label is new:
    The front label is new and shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (same device type):
    Check that the front label is new and has no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Mechanical decommissioning procedure:
- Cut off the front label corners to expose the screws.
- Scratch the front label, for example, with a flat screwdriver.

A.2.2 Potted device

Security properties:
- The device hardware except the connectors and LEDs is potted with a hard casting compound.
- Trying to open the device leaves signs of mechanical processing.

Tampering evidence:
- The casting compound, the connectors, or the LEDs show signs of mechanical processing, like scratches, boreholes or partial application of new casting compound.

Check procedures:
- New device:
  - Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Repaired device back from manufacturer:
  - If the device is the same:
    Check the condition of the casting compound, the connectors, and the LEDs against the recorded condition.
    The condition of these components shall only deviate minimally from the recorded condition and show no signs of mechanical processing.
  - If the device has been replaced (same device type):
    Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall be new and show no signs of mechanical processing.
  - If the device has been replaced (other device type):
    Check according to the new device type's security seal.

Mechanical decommissioning procedure:
- Deform the connectors and LEDs with a heavy tool, for example, with a hammer.

A.2.3 Security stickers

Security properties:
- The security stickers used by the device manufacturer have the following properties:
  - Incisions that impede the unnoticed removal of a sticker
  - Self-delaminating layers that impede the unnoticed removal and re-application of a sticker
  - A hologram (optional) that impedes copying or counterfeiting a sticker
  - The stickers are non-standard, unique stickers that cannot be acquired on the open market.
- The security stickers can be in the following locations on the device:
  - The stickers cover screws necessary to open the device.
  - The stickers overlap (that is, mechanically connect) removable device parts.

Note:
For devices that offer customer-side modularity, the operator is responsible for applying their own, customer-specific, security stickers once the hardware configuration is complete.
The customer-specific security stickers shall offer appropriate security, for example, by having the properties of the manufacturer's stickers given above.
The customer-specific security stickers shall be applied in appropriate locations, for example, in the locations given above.

Tampering evidence:
- The security stickers show cutaways, cuts, scratches, wrinkles, folds, delamination, or (if applicable) a missing, changed or incomplete hologram.

Check procedures:
- New device:
  - Check the front panel and the stickers:
    The stickers shall be new and show no cutaways, cuts, scratches, wrinkles, folds, or delamination, but an intact hologram (if applicable).
  - For devices that offer customer-side modularity:
    Once the hardware configuration is complete, apply your own, customer-specific stickers.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the stickers.
    The stickers shall show no cutaways, cuts, scratches, wrinkles, folds, delamination, but an intact hologram (if applicable).
- Repaired device back from manufacturer:
  - If the device is the same:
    Check the condition of the stickers against the recorded condition.
    Both should only deviate minimally.
  - If the device has been replaced (same device type):
    Check the condition of the stickers against the recorded condition.
    The stickers shall be new and show no cutaways, cuts, scratches, wrinkles, folds, or delamination, but an intact hologram (if applicable).
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Mechanical decommissioning procedure:
- Destroy the security stickers:
  - Cut the stickers along the edge where the front and side panels of the device meet, for example with a screwdriver.
  - Pull off the loose parts of the stickers.
- Mark the front panel as decommissioned:
  - Scratch the front panel, for example with a flat screwdriver.

B Password strength and policy guide

Note:
This chapter is informational only.

A strong password is hard to break by both a brute-force attack and a dictionary attack. "Hard to break" means that the mean time an attack needs to succeed is higher than a specified time.

A strong password is at the same time reasonably convenient to memorize without the need to write it down or use a password management application.

To make a quantitative statement about which password policy satisfies your specific situation, the following values have to be at hand:
- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity, see below)

When these values are given, you can look up a password policy that satisfies your requirements (see on page 150 “Password policy lookup tables (quantitative)”).

For a more in-depth approach, the following chapters provide a short introduction to the key concepts of password strength.

The following topics are covered in this chapter:
- A detailed discussion of password classes and password strength
- The suggestion to prefer low-complexity passwords over high-complexity passwords and the reasons for the suggestion
- A general discussion of password policies and the resulting password schemes
- A detailed discussion of password schemes and the resulting password strength
- A precise guide to a recommended password policy, based on quantitative considerations

The following topics are outside the scope of this document:
- The automated generation of strong passwords
- The secure administration and distribution of passwords
- A possible password change policy
- The handling of password breaches or leaks
- The human aspects for passwords, like social engineering

B.1 Password classes

Note:
The terms used in this chapter, like "password complexity", will be explained in the course of the sub-chapters.

Passwords can be grouped into 2 classes:
- High-complexity passwords:
  - High-complexity passwords have a minimum length.
  - They must consist of characters of the following character types: lowercase characters, upper case characters, digits and special characters.
  - Often, at least one character of each type is required.

  - The resulting password must not contain any word that can be found in a dictionary.
  - The minimum length required by the respective password policy is relatively low.
  - High-complexity passwords are relatively hard to memorize, especially if they are long.
  - Examples are "bZ1/Yc0$", "L{3}qz9M_k", or "*%Gr.43FD7xw".
- Low-complexity passwords:
  - Low-complexity passwords consist only of lowercase characters, for example, as a group of words.
  - Other character types are possible but not required.
  - The resulting password typically contains words that can be found in a dictionary.
  - The words in the password may be separated by a special character like "-".
  - The minimum length required by a specific password policy is higher than for high-complexity passwords of comparable strength.
  - Despite their greater length, low-complexity passwords are relatively easy to memorize.
  - Therefore, and counter-intuitively, low-complexity passwords may offer higher practical strength than high-complexity passwords.
  - Examples are "barrel-hamlet-famous", "imagine.lioness.knuckle.manager", or "natality painless yeomanry obligate quenched".

Note:
At the time of writing, high-complexity passwords are in more common use than low-complexity passwords. The reason is that users tend to create short passwords and common password policies favor high-complexity passwords.

B.2 Password policies

A password policy typically has the following properties:
- It stipulates quantitative requirements:
  - The minimum password length
  - The allowed character types from which the password characters shall be taken (typically, the types are: lowercase characters, uppercase characters, digits, and special characters)
  - The minimum number of characters of each type
- It stipulates qualitative requirements:
  - The password must not contain any words from a given dictionary
- It stipulates time requirements:
  - The chosen password must be changed after a specified max. time period.

In essence, a password policy indirectly stipulates:
- The minimum password strength
- The password class (high- or low-complexity)

Notes:
- A password policy is a template for developing password schemes that satisfy given minimum requirements.
- The maximum time after which a password shall be changed has no effect on the password strength.
  - A required interval for changing a given password is reasonable if you assume that your password will be or has already been breached during the interval and you have not noticed.
  - This requirement also takes care of the possibility that a password may have leaked to an attacker.
  - While requiring a maximum interval for changing a password is common for many office and Internet IT systems, embedded systems typically do not enforce a regular password change by themselves.
  - For a system not enforcing regular password change, you can still minimize the probability of an unnoticed, successful password attack by specifying the required attack resistance time much higher than the expected lifetime of the system. This can be accomplished by setting up a strong password policy.

In the following table, the minimum values stipulated by some example password policies are given, along with an exemplary description of the policy results.

Table 22: Password policy examples and qualitative password strength

Min, password length	Min no. of lowercase chars	Min no. of uppercase chars	Min no. of digits	Min no. of special chars	Password type and qualitative strength
6	1	1	1	1	High-complexity password, low strength ⚠
8	1	1	1	1	High-complexity password, medium strength
10	1	1	1	1	High-complexity password, higher strength
24	0	0	0	0	Low-complexity password, high strength

Note:
The qualitative password strength description in the above table assumes low security requirements. Your assessment may associate lower password strengths with the password policy examples given above. The password strength is considered in quantitative detail in the following chapters.

B.3 Password schemes

A password scheme results from a given password policy and has the following properties.

- A password scheme uses a specific password policy as a template.
- A specific scheme is one of several possible schemes that satisfy a specific policy.
- Different schemes can generate passwords of different strength.
- A minimum scheme barely satisfies the policy requirements, but no more.
  Consequently, a password following a minimum scheme has a minimum strength.
- An extended scheme exceeds the policy's minimum requirements.
  A password following an extended scheme typically has larger strength than a password following a minimum scheme but in practice, extended schemes are rarely chosen by users.

Note:
In keeping with a conservative (skeptical) security approach, all password schemes discussed in this chapter are minimum schemes (see on page 136 "Conservative assumptions about users"). This helps ensure that the strength of an actual password meets or exceeds the required strength despite the minimum scheme it is based on.

B.4 Password attack strategies

For an attacker who aims to gain login access by breaking the account password, there are 2 basic attack strategies:

- Dictionary attack:
  - A dictionary attack is highly efficient if a password is in the dictionary (list) of passwords the attacker knows.
  - This applies in particular to frequently used passwords on lists that are available on the Internet.
  - For maximum efficiency, these lists are ordered with the most frequently used passwords first, for example "123456", "secret", "password1", or "Password.1".
  - If the real password is not in the attacker's dictionary, the dictionary attack will fail.
- Brute-force attack:
  - A brute-force attack is necessary for highly random passwords that do not contain any word from a dictionary.
  - This attack basically tries all possible passwords for a given password scheme.
  - The number of possible passwords roughly grows exponentially with the password length.
  - A brute-force attack takes much longer than a dictionary attack but will eventually succeed, given enough time and a lack of mitigating factors.

Note:
An attacker can also try to steal a password or provoke a password leak, for example, by social engineering. Thus, for mitigation, passwords must be guarded well. These aspects are outside the scope of this document.

B.5 Basic security assumptions

In keeping with the conservative security approach, this main chapter makes qualitative assumptions about:

- Attackers
- Users
- The attack context

B.5.1 Aggressive assumptions about attackers

- An attacker looks for the most efficient way to gain access.
- To accomplish this, they will first look for the weakest aspects (most frequent existing vulnerabilities) of the target. This may make login attempts entirely redundant from the viewpoint of the attacker.
- If a login attack is necessary, they may use the following strategy:
  - They try to find an interface or a protocol that does not explicitly rate-limit attacks.
  - They try the most frequently used passwords first, so they will start with a dedicated dictionary attack. That is, they try a list of known frequent passwords.
  - If the dictionary attack does not succeed, they may either give up or switch to a brute-force attack.
  - They may either know the username of the account, or assume a low number of frequent usernames and perform a dictionary attack against the username. That is, they may use a list of frequent usernames. They may also try those usernames first that are typically associated with administrator privileges.
- If they do not succeed with the given target, interface, and protocol, they will switch to another target, interface, or protocol.

Conclusion: From a system view, closing or mitigating the weakest vulnerabilities first is necessary.

B.5.2 Conservative assumptions about users

- When users have the choice of either creating their own password or accept a password suggestion randomly generated by a system, users will tend to create their own password. The consequences may be:
  - Given a liberal high-complexity password policy, a user-chosen password will in practice almost always be weaker than a randomly suggested password (see details below).
  - When forced to follow a strict high-complexity password policy, users may experience problems in memorizing the password and thus may tend to either write it down or use an unapproved password management application.
- When choosing a password, users will create the easiest possible password, for example, using only lowercase characters.
- When a password policy enforces a minimum length, users will tend to use an as short as possible password of lowercase characters that just satisfies the minimum length.
- When a password policy also enforces a minimum number of other character types, users will create the easiest possible password that barely satisfies the password policy. That is, they tend to use a minimum scheme (see on page 134 “Password schemes”):
  - When at least one uppercase characters is required, users will tend to use only one uppercase character, and may put it at the start.
  - When at least one digit is required, users will tend to use only one digit. They may put it at the end or replace a single letter with a digit (for example "A" -> "4").

  - When at least one special character is required, users will choose from a limited pool of special characters, and will not exhaust the possible pool of special characters.
  - The properties of user-chosen passwords may make these passwords more vulnerable to a dictionary attack, and possibly even to a brute-force attack.
- When given the choice of either creating a short, complex password or a longer, less complex password, users will tend to choose a short, complex password that barely satisfies the required password policy, although a longer, even less-complex password may be stronger.
- When asked to create a long password, users will also create a password that barely satisfies the required password policy.

Conclusion: From a system view, a password policy needs to be strong enough so passwords created according to the resulting minimum scheme have sufficient strength.

B.5.3 Conservative assumptions about the attack context

- The username of an account under attack is assumed to be already known to the attacker. Username examples are "user", "admin", or "administrator".
  This essentially eliminates the effort and time for guessing the username and is a typical skeptical security assumption.
- The attack rate may or may not be limited by system settings. In the worst case, it is unlimited. In the absence of any network concept that detects anomalies or intrusions, this in essence means that the attacker is able to sustain a high attack rate for a long time.
- When performing a dictionary attack, the attacker has insider knowledge, that is, they already know the dictionary the password generation system uses to suggest long, low-complexity passwords.

Note:
We will shortly see that the seemingly paranoid assumption of an attacker knowing the complete password dictionary is not really a security problem. That is, a system-suggested, sufficiently long, low-complexity password can be both stronger and also easier to memorize than a typical high-complexity password of similar strength. This may seem counterintuitive but can be proven quantitatively, while assuming reasonable and even skeptical conditions.

B.6 Quantitative password strength

B.6.1 High-complexity passwords

The strength of a high-complexity password can be quantified as the number of possible passwords for a given scheme.

Note:
The preferred attack method to crack a high-complexity password is a brute-force attack. A good, high-complexity password will not give in to a dictionary attack.

For a high-complexity password of a given scheme, the number of possible passwords depends on the character type (more precisely: on the size of the pool from which the respective character is taken) and on how many characters of the given type appear.

The expected password strength depends on the assumptions how a password is created:
- Optimistic password strength:
  - Only truly random passwords have the highest possible expected information content.
  - Reasonable passwords of this type typically must be generated by an application.
  - Caveat: User-chosen high-complexity passwords typically have significantly less "randomness" (that is, entropy) and therefore tend to be weaker.
- Skeptic password strength:
  - When users are faced with a password policy, users will tend to make up a password scheme that barely satisfies the policy, that is, they will choose a minimum scheme.
  - User-chosen passwords therefore tend to have lower-than-possible strength.
  - The reason is that people tend to use certain characters more often than others.
  - For example, the character "e" appears in an general, English-language text with a probability of approx. 12.5% (1/8) and not with the probability of 3.8% (1/26).
  - To account for the unevenly distributed character frequencies to and pursue a skeptic approach, we can calculate with a smaller pool size than 26, for example, by assuming 8 (this approximates the frequency of the most frequent character, here, "e").
  - Similarly, to account for the unevenly distributed digit and special character frequencies, we can also calculate with a smaller pool size, for example, by also assuming 8.

The number of possible different high-complexity passwords of a given scheme is therefore:

$$N_{ph} = L^l \times U^u \times D^d \times S^s$$

Where:
- N_{ph}: Number of possible high-complexity passwords
- L: Pool size of lowercase characters (constant)
- l: Number of lowercase characters in the password (variable)
- U: Pool size of uppercase character (constant)
- u: Number of uppercase characters in the password (variable)
- D: Pool size of digits (constant)
- d: Number of digits in the password (variable)
- S: Pool size of special characters (constant)
- s: Number of special characters in the password (variable)

We see that the password strength grows with the length of the password. Unsurprisingly, we see that adding more characters, digits or special characters to an existing password makes the resulting password stronger.

Note:
A simple generator for high-complexity passwords, following a minimum password scheme, might in fact sometimes suggest passwords like "123456", "abcdef" or "secret". These passwords are weak because they most likely are in an attacker's dictionary. The skeptic probability for a randomly generated password to be like one of the given examples is $8^{-6} \approx 3.81 \times 10^{-6}$. Because there are many known weak passwords, the probability of a randomly generated password matching one of the known weak passwords is considerable – possibly too high to be accepted. Therefore, **checking a system-suggested or user-chosen high-complexity password against a list of known weak passwords can be regarded as mandatory.**

Example (optimistic password strength)

An example password policy requires a length of 8 characters, with at least one lowercase character, one uppercase character, one digit, and one special character.

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy: The user chooses to use 5 lowercase characters, one uppercase character, one digit, and one special character.

Table 23: High-complexity password components, optimistic strength

Character class ID	Class description	Pool characters	Assumed pool size
L	Lowercase characters	a-z	26
U	Uppercase characters	A-Z	26
D	Digits	0-9	10
S	Special characters	!"#$%&()*+'.-/:;	16[1]

1. The special character pool size is given as 16 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The optimistic number of possible passwords of this scheme is therefore:

$$N_{pho} = 26^5 \times 26^1 \times 10^1 \times 16^1 = 49{,}426{,}524{,}160 \approx 4.94 \times 10^{10}$$

Where:
- N_{pho}: Number of possible high-complexity passwords, optimistic approach

Note:
Modifying an existing password by replacing lowercase characters by digits or special characters can actually make the password weaker. This seems to contradict the recommendation to include digits and special characters in a password. The explanation is that replacing lowercase characters by digits or special characters only helps against dictionary attacks, not against brute-force attacks. The recommendation to include digits and special characters is based on the assumption that the password prior to the modification is vulnerable to a dictionary attack. That again means that the original password wasn't a high-complexity password to begin with.

Example (skeptic password strength)

Table 24: High-complexity password components, skeptic strength

Character class ID	Class description	Pool characters	Assumed, reduced pool size
L	Lowercase characters	a-z	8
U	Uppercase characters	A-Z	8
D	Digits	0-9	8
S	Special characters	!#$&+.-/ (example)	8

Assuming the same password scheme as above, but with a reduced pool size of 8 for each character type to account for frequent characters or digits like "e", "1", or ",", the skeptic number of possible passwords of this scheme is therefore:

$N_{phs} = 8^5 \times 8^1 \times 8^1 \times 8^1 = 8^8 = 2^{24} = 16{,}777{,}216 \approx 1.67 \times 10^7$

Where:
- N_{phs}: Number of possible high-complexity passwords, skeptic approach

We see that the skeptic password strength is much smaller than the optimistic strength.

B.6.2 Low-complexity passwords

The strength of a low-complexity password can also be quantified as the number of possible passwords for a given scheme.

Note:
The preferred attack method to crack a low-complexity password is a dictionary attack. A brute-force attack is possible but practically futile. Given the bigger length of a low-complexity password (for example, 24 lowercase characters), the skeptic number of possible passwords is on the order of 10^{21}. The optimistic number of possible passwords is even on the order of 10^{33}.

A low-complexity password contains words from a dictionary (word list). The strength of a low-complexity password depends on the following aspects:
- It strongly depends on the number of words in the password.
- It moderately depends on the size of the dictionary.
- It marginally depends on the detailed rules how passwords are chosen from the dictionary.
- It is virtually independent of the word length as long as a minimum length is maintained.

For the sake of security skepticism, let's make 4 conservative assumptions:
- The dictionary from which the words are taken (for example, by a password-generating application) has only straightforward size (for example, only 2,048 entries).
- The entire dictionary is already known to the attacker. This is a very conservative assumption.
- Words from the dictionary shall be selected only once.
  - This excludes the equivalent of weak passwords like "111111" or "aaaaaa".
- Words selected from the dictionary shall not be adjacent to any of the words already selected.
  - This excludes the equivalent of weak of passwords like "123456", "654321, "abcdef" or "fedcba".

We will shortly see that a low-complexity password scheme following these assumptions still results in passwords of high skeptic strength. The optimistic strength for a low-complexity password does not need to be examined in detail because such a password would in essence describe a long, high-complexity password, against which a dictionary attack is practically futile.

There is one additional condition that needs to be satisfied:

- The minimum word length shall be high enough to contain much more possible words than there are words in the dictionary.
  - This ensures that the list entropy is not undermined by a low word entropy (we will discuss entropy shortly, (see on page 147 “Password entropy”)). This condition is easily satisfied by a password policy requiring a minimum number of characters.

Table 25: Low-complexity password properties

Parameter ID	Parameter	Description
S	Dictionary size	Number of words in the dictionary
w	Number of words	Number of such words in the password.

The approximate number of possible different low-complexity passwords of a given scheme is therefore:

$N_{plo} \approx S^w$

Where:

- N_{plo}: Number of possible low-complexity passwords, optimistic approach
- S: Dictionary size
- w: Number of words used in the password

Note:
For w ≥ 2, the above equation gives a slightly optimistic strength. Compared to the exact value, assuming a dictionary size of 2,048 and 6 words, it is off by +2.3%. For fewer words, the deviation is lower. For w = 1, the equation gives the correct strength.

The exact equation is:

$N_{ple} = S \times (S - 3) \times (S - 6) \times \ldots \times (S - 3 \times (w-1))$

Where:

- N_{ple}: Number of possible low-complexity passwords, exact approach

Note:
The multipliers S - 3, S - 6 etc. stem from the fact that the choice of the first word has S possibilities but the choice of the 2nd word has only (S - 3) possibilities. This is because the first word chosen, its immediate predecessor as well as its immediate successor shall not be chosen again, according to the last of the above given skeptic assumptions.

This unwieldy formula can safely be approximated by a skeptic approximation, that is, by dividing the result of the approximate, optimistic equation by 2:

$N_{pls} = S^w / 2$ (for w ≥ 2)

Where:

- N_{pls}: Number of possible low-complexity passwords, skeptic approach

Example

Note:
In keeping with the conservative security approach, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy. The word list is assumed to contain only 2,048 words. The minimum word length is 6.

An example password policy requires a length of 24 characters (therefore 4 words with 6 characters minimum length each), with at least 1 lowercase character. Uppercase characters, digits, and special characters are possible but not required. Given the choice of making up their own password, a user chooses the password "barrel-hamlet-famous-staple", possibly with the help of an application.

The number of possible passwords of this scheme is therefore:

$N_{pl} = 2{,}048^4 / 2 = 2^{43} = 8{,}796{,}093{,}022{,}208 \approx 8.79 \times 10^{12}$

Note:
Despite the above, conservative assumptions, the low-complexity password strength in this example is much higher than for the aforementioned high-complexity password examples. This holds even if we compare the conservative strength of the low-complexity password to the optimistic strength of the high-complexity password.

B.7 Attack resistance time (quantitative)

The theoretical (but impractical) resistance to an attack can be calculated as the maximum time the password withstands an attack until it is broken with 100% probability.

This time can be calculated as the number of necessary attacks, divided by the attack rate:

$T_{sb} = N_a / r_a$

Where:
- T_{tb}: Theoretical max. time to 100% probable password breach, in seconds
- N_a: Number of necessary attacks
- r_a: Attack rate (in attacks per second)

Of course, accepting a 100% probability for a password breach is a weak concept. In practice, a 50% probability is often assumed instead because the assumption of 50% makes the equations a bit easier.

The practical resistance to an attack is typically calculated as the mean time the password withstands the attack until it is broken with 50% probability. This is half the time for a 100% probability breach:

$T_{sp} = N_a / r_a / 2$

Where:
- T_{pb}: Mean time to practical (50% probable) password breach

The (unsurprising) result is that the attack resistance time increases with a higher number of possible different passwords and decreases with higher attack rate.

The (unsurprising) conclusion is: To make a login password as strong as possible, you have 2 possibilities, and you can combine these:
- Specify a strong password policy by setting up an appropriate password policy, either for high-complexity or for low-complexity passwords, thus enabling strong-enough resulting minimum schemes.
- Wherever possible, set up a login policy to lower the effective attack rate for a given interface and protocol.

B.7.1 Examples, unmitigated attack rate

In keeping with the conservative security approach, the assumed attack rate is high and unmitigated, so we assume 1,000 attacks per second. An example for such a possible high rate is an attack using SNMPv3 get requests. SNMP has no obvious means of attack rate mitigation. We accept a 50% probability of a breach.

For the password example strengths in the previous chapters, the mean attack resistance time is:

Table 26: Attack resistance time for different password scheme examples, for an unmitigated attack rate

Password class	Approach	Password strength	Unmitigated attack rate per second	Attack resistance time	
				in seconds	in usual units
High complexity	Optimistic	4.94×10^{10}	1,000	2.47×10^{7}	9.53 months
	Skeptic	1.67×10^{7}	1,000	8.38×10^{3}	2.33 hours
Low complexity	Skeptic	8.79×10^{12}	1,000	4.39×10^{9}	139 years

We see that despite the very conservative assumptions for the low-complexity password, the low-complexity password results in a much attack higher attack resistance time than a high-complexity passwords. This holds even if we compare to the optimistic case of the high-complexity password.

B.7.2 Attack rate mitigation

The rate (strength) of a dictionary or brute-force attack can be given as the number of login attempts per second.

The lower the attack rate, the longer it takes to reach the mean number of attempts until the password is accepted.

Let's assume that an attacker is capable of delivering many attacks per second to a certain interface and protocol (an attack rate ≥ 1 / sec = 3,600 / hour). How this affects the system under attack depends on if the system has mitigating parameters set up. Examples for protocols offering such mitigation parameters are HTTPS and SSH.

There are 2 settings that provide mitigation:
- The maximum number of successive failed login attempts until the system enforces a waiting time
- The enforced waiting time the system has set up.

The assumed high attack rate is thus effectively reduced to:

$r_{am} = n_{sf} / t_w$

Where:
- r_{am}: Mitigated attack rate
- n_{sf}: Number of successive failed login attempts
- t_w: The enforced waiting time

We see that the mitigated attack rate only depends of the mitigating parameters' values, not on the high attack rate originally assumed. This makes these mitigations parameters particularly effective.

Note:
This approximate equation is slightly skeptic. The real mitigated attack rate is slightly lower.

Mitigation examples

Skeptic example: An example system is set up to ignore logins after 10 successive failed login attempts. This is a fairly high value, assuming users tend to value convenience. After the condition triggers, the target system enforces a one-minute wait time (a fairly low value, also convenient) and ignores any login attempts during that time. What is convenient for the users, is regarded skeptically from a security perspective.

r_{am} = 10 / 1 min = 10 / min = 600 / hour.

Optimistic example: A system ignore logins after already 5 successive failed login attempts (a smaller value) and then enforces a 2-minute wait time (a larger value). These values may be more inconvenient for the users, but are regarded as more desirable from a security perspective.

r_{am} = 5 / 2 min = 2.5 / min = 150 / hour.

We see that setting up reasonable attack mitigation parameters can significantly lower the effective attack rate, often by an order of magnitude or more.

B.7.3 Examples, mitigated attack rate

The login with the protocols HTTPS and SSH provides mitigating parameters. In keeping with the conservative security approach, the assumed mitigated attack rate is relatively high because the mitigation parameters were chosen to be convenient for the users. So we assume 600 attacks per hour (that is, 10 per minute or 1/6 per second).

For the password example strengths in the previous chapters, the mean attack resistance time is:

Table 27: Attack resistance time for different password scheme examples, for a mitigated attack rate

Password class	Approach	Password strength	Mitigated attack rate per second	Attack resistance time	
				in seconds	in usual units
High complexity	Optimistic	4.94×10^{10}	1/6	1.48×10^{11}	4,698 years
	Skeptic	1.67×10^{7}	1/6	5.03×10^{7}	1.59 years
Low complexity	Skeptic	8.79×10^{12}	1/6	2.63×10^{13}	836,194 years

Note:
We see that attack rate mitigation can be very effective in raising the provided attack resistance time. However, this only applies to protocols that offer the said mitigation parameters. In the worst case (that is, with a skeptic approach), we still have to assume the unmitigated attack rate, as may be the case for the SNMPv3 protocol.

B.8 Required attack resistance time (quantitative)

For a required mean attack resistance time, an assumed attack rate, and a specific, accepted breach probability, we can calculate the required password strength:

$N_{pr} = T_{ar} \times r_a \times (1 / P_b)$

Where:
- N_{pr}: Required password strength
- T_{ar}: Required attack resistance time
- r_a: Assumed tack rate (in attacks per second), either mitigated or unmitigated
- P_b: Accepted breach probability when the required mean attack resistance time has elapsed

The (unsurprising) result is that the required password strength increases with a higher required attack resistance time, with a higher assumed attack rate and with a lower accepted breach probability.

The commonly accepted breach probability is 50%. This gives the simplified equation:

$N_{pr} = T_{ar} \times r_a \times 2$

Note:
Your situation may require a lower breach probability than 50%. In this case, use the former equation.

B.9 Password entropy

The strength of a given password scheme can be expressed as:
- Possibilities (symbol N): The number of possible different passwords
- Entropy (symbol H): The expected information content for a random number in the range 1…N. (The symbol H is the uppercase Greek letter Eta.)

Entropy in the context of information theory has the following properties:
- It has the unit "shannon" (short: "Sh"). It can be non-integer.
- Its value can be interpreted as the minimum number of bits required to hold a number in the range 1…N. If the entropy value is non-integer, it has to be rounded up to the nearest integer to give the minimum number of bits.

The password entropy is a more convenient way of representing the password strength than the number of possible passwords. Whereas the typical number of possible passwords for a given scheme is > 10^6, the entropy of a reasonable strong password typically is in the range 20…45. The reason is that there is a logarithm involved.

The entropy can be calculated from the password strength:

$H_p = \log_2 (N_p)$

Where:
- H_p: The password entropy (min. number of bits required to represent N_p)
- $\log_2$: The Logarithm function to the base of 2
- N_p: The password strength (as the number of possibilities)

The calculated entropy of a given password strength can be non-integer number. In keeping with security skepticism, the number of bits associated with the entropy is rounded to the nearest integer in the following way:
- For the entropy required for a certain password scheme, the number of bits is rounded up.
- For the entropy provided by a certain password scheme, the number of bits is rounded down.

Generally, there are 3 basic types of entropy in relation to password strength:
- The **Shannon entropy** H_1 represents the **detailed** approach.
- The **max. entropy** H_{max} represents the **optimistic** approach.
- The **min. entropy** H_{min} represents the **skeptic** approach.

As we follow the skeptic approach, we only deal with the min. entropy H_{min}.

In this main chapter, using only the min. entropy is incorporated by the following approach:
- For high-complexity passwords, the applied skeptic pool size for any character type is chosen to be only 8, instead of 26, 10, or 16 (or even 32). This results in 3 sh per character.
- For low-complexity passwords:
  - Only the size of a known dictionary (for example, 2,048) is taken into account. This results in a dictionary entropy of 11 sh.
  - The length of individual words is ignored, only a minimum length is required (for example, 6).
  - The strength of a given password scheme is calculated conservatively, by dividing the approximate formula's value by 2, if the number of words in the password is ≥ 2.

B.10 Calculating the required password entropy

For a required mean attack resistance time, a specified attack rate, and a specified, accepted breach probability, we can calculate the required password strength as the required password entropy.

Given the above equation $N_{pr} = T_{ar} \times r_a \times (1 / P_b)$ (see on page 146 “Required attack resistance time (quantitative)”), the entropy is:

$H_{prb} = \log_2 (N_{pr}) = \log_2 (T_{ar} \times r_a \times (1 / P_b))$

$H_{prb} = \log_2 (T_{ar} \times r_a) - \log_2 (P_b)$

Where:
- H_{prb}: Required password entropy for the required breach probability P_b
- N_{pr}: The required password strength (as the number of possibilities)
- T_{ar}: Required attack resistance time
- r_a: Assumed attack rate (in attacks per second), either mitigated or unmitigated
- P_b: Accepted mean breach probability when the required mean attack resistance time has elapsed

In theory, a breach probability of 100% is possible (although mostly not accepted). This leads to:

$H_{pr100} = \log_2 (T_{ar} \times r_a / 1) = \log_2 (T_{ar} \times r_a)$

Where:
- H_{pr100}: The theoretically required password entropy for a breach probability of 100%

In literature, a breach probability of 50% is often accepted. This leads to:

$H_{pr50} = \log_2 (T_{ar} \times r_a / 0.5) = \log_2 (T_{ar} \times r_a) + \log_2 (2) = \log_2 (T_{ar} \times r_a) + 1$

$H_{pr50} = H_{p100} + 1$

Where:
- H_{pr50}: The required password entropy for a breach probability of 50%

We see that an accepted breach probability of 50% raises the required password entropy by 1 sh, in comparison to the theoretical (and practically unacceptable) breach probability of 100%.

The generalized formula for a required password entropy, assuming a specified breach probability is:

$H_{prb} = H_{p100} - \log_2 (P_{br}) = H_{p100} + | \log_2 (P_{br}) |$

Where:
- H_{prb}: The required password entropy for an arbitrary breach probability
- P_{br}: The required breach probability (< 1) within the attack time.
- $| x |$: the absolute value of x (always >0 even if x <0)

We see that an arbitrarily required breach probability < 100% simply adds more required entropy to the theoretical (and undesirably low) password entropy H_{pr100}.

Note:
Because $P_{br} < 1$, $\log_2 (P_{br}) < 0$ and therefore $-\log_2 (P_{br}) > 0$.

B.11 Password policy lookup tables (quantitative)

To find a password policy that quantitatively meets the specified requirements, we need the following values at hand:

- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity)

We can then look up the required password policy, using a series of tables:

B.11.1 Password entropy lookup tables

Table input:

- T_{ar}: Required attack resistance time
- r_a: Assumed attack rate

Table output:

- H_{pr50}: Required password entropy for an accepted breach probability of 50%

Table 28: Lookup table for required password entropy (in Sh, rounded up)

Required attack resistance time T_{ar}	Assumed attack rate r_a					
	1 / min	10 / min	1 / sec	10 / sec	100 / sec	1,000 / sec
1 day	12	15	18	21	25	28
1 week	15	18	21	24	27	31
1 month	17	20	23	26	29	33
1 year	21	24	26	30	33	36
10 years	24	27	30	33	36	40
100 years	27	30	33	36	40	43
1,000 years	30	34	36	40	43	46

Password entropy lookup table for < 50% breach probability

Table input:
- P_{br}: Required max. breach probability after the acceptable mean attack time has elapsed

Table output:
- H_{ab}: Required additional password entropy for breach probability P_{br}

Table 29: Lookup table for additional required password entropy (in Sh, rounded up)

Accepted max. breach probability P_{br}	Required additional password entropy H_{ab}
50%	0
10%	3
1%	6
1‰ (10^{-3})	9
100 ppm (10^{-4})	13
10 ppm (10^{-5})	16
1 ppm (10^{-6})	19
100 ppb (10^{-7})	23
10 ppb (10^{-8})	26
1 ppb (10^{-9})	29

For < 50% breach probability, add the required password entropies from the 2 tables:

$H_{prb} = H_{pr50} + H_{ab}$

Where:
- H_{prb}: Required password entropy for a breach probability P_{br} < 50%
- H_{pr50}: Required password entropy for standard breach probability of 50%
- H_{ab}: Additional required entropy for an accepted breach probability < 50%

B.11.2 Password policy lookup table, low-complexity passwords

Table input:
- H_{prb}: Required password entropy for the required breach probability

Constants:
- S: Dictionary size, assumed to be 2,048
- L_w: Minimum length of any word in dictionary: assumed to be 6

Table output:
- n_w: Minimum number of words required by the password policy
- n_c: Minimum overall number of characters required by the password policy

Table 30: Lookup table for password policy (for low-complexity passwords)

Required password entropy (H_{prb})	Required no. of words n_w	Required no. of characters n_c	Required no. of any character type	Provided entropy (skeptical)
12…21	2	**12**	0	21
22…32	3	**18**	0	32
33…43	4	**24**	0	43
44…54	5	**30**	0	54
55…65	6	**36**	0	65
66…75	7	**42**	0	76

Notes on low-complexity passwords (see on page 140 “Low-complexity passwords”):

- **The use of only lowercase characters permitted.** This is a conservative approach. Other character types are possible but will not increase the provided password entropy.
  - Reason: The entropy of a low-complexity password is already calculated in a very conservative way by the dictionary entropy.
- **The password policy need not require a minimum number of other character types.**
  - This is why 0 is given as the requirement in the table above.
- The number of words in the password is a required minimum.
  - A higher word count will **significantly** increase the password entropy.
- The dictionary size is assumed to be 2,048 (11 sh of entropy). This is a conservative approach.
  - Higher dictionary sizes will result in **moderately** higher password entropy. For example, a dictionary size of 4,096 represents 12 sh of entropy.
- The detailed rules how passwords are chosen from the dictionary, have a **marginal** effect on the entropy: The stricter the rules, the lower the skeptic entropy.
- The minimum word length is assumed to be 6. This is a conservative approach. Higher minimum word lengths will **not** increase the password entropy.
  - Reason: An individual word’s entropy must be much higher than the dictionary entropy, the key parameter for a low-complexity password. Only then, the dictionary entropy is unimpaired by the word entropy.
  - Calculation: For 11 sh of dictionary entropy and 3 sh skeptic entropy for a lowercase character, we need words with at least 4 characters. To make a conservative approximation, we chose a word length of 6 which represents 18 sh of skeptic entropy.

B.11.3 Password policy lookup table, high-complexity passwords

Table input:

- H_{prb}: Required password entropy for the accepted breach probability

Constants:

- L: Pool size of lowercase characters (assumed to be 8)
- U: Pool size of uppercase character (assumed to be 8)
- D: Pool size of digits (assumed to be 8)
- S: Pool size of special characters (assumed to be 8)

Table output:
- n_c: Required total number of characters in the password

Table 31: Lookup table for password policy (for low-complexity passwords)

Required password entropy (H_{prb})	Req. total chars (n_c)	Req. lowercase chars (l)	Req. uppercase chars (u)	Required digits (d)	Req. special chars (s)
12…24	**8**	**1**	**1**	**1**	**1**
25…27	**9**	**1**	**1**	**1**	**1**
28…30	**10**	**1**	**1**	**1**	**1**
31…33	**11**	**1**	**1**	**1**	**1**
34…36	**12**	**1**	**1**	**1**	**1**
37…39	**13**	**1**	**1**	**1**	**1**
40…42	**14**	**1**	**1**	**1**	**1**
43…45	**15**	**1**	**1**	**1**	**1**
46…48	**16**	**1**	**1**	**1**	**1**
49…51	**17**	**1**	**1**	**1**	**1**
52…54	**18**	**1**	**1**	**1**	**1**
55…57	**19**	**1**	**1**	**1**	**1**
58…60	**20**	**1**	**1**	**1**	**1**
61…63	**21**	**1**	**1**	**1**	**1**
64…66	**22**	**1**	**1**	**1**	**1**
67…69	**23**	**1**	**1**	**1**	**1**
70…72	**24**	**1**	**1**	**1**	**1**
73…75	**25**	**1**	**1**	**1**	**1**

Note:
The suggested password length starts with 8. The required password entropies in the range 12…21 sh could theoretically be satisfied with a shorter password length 4…7. These short password policies are not suggested because, from a skeptic security perspective, the resulting passwords are highly susceptible to dictionary attacks as well as brute-force attacks.

Note on the required numbers of lowercase characters (l), uppercase characters (u), digits (d), and special characters (s):
- All characters types are required to appear a minimum number of times in the password policy, for example, 1 per type.
- Requiring a higher minimum number for the digits or special characters will **not** yield higher password entropy because the skeptic assumptions about the pool sizes for the character types are the same.
- A password policy should therefore allow for the other characters but only require a minimum number of 1.
- Theoretically, a minimum number of 0 would also suffice if the password were strictly random, for example, created by an application.
- In practice, with user-chosen passwords, this is not viable: Users may understand such a policy as an invitation to create weak passwords, for example, consisting only of lowercase characters or digits, like "abcdefgh" or "12345678".

C Considerations for manually entered keys

Note:
This chapter is informational only.

Symmetric cryptography keys can be considered special cases of high-complexity passwords. Therefore, some aspects for passwords also apply to symmetric cryptographic keys.

Note:
This chapter deals exclusively with keys for symmetric cryptography. A key usually is for symmetric cryptography if the same key is used for encryption as well as for decryption.
For asymmetric cryptography, the comparison of keys to passwords does not apply. A key usually is for asymmetric cryptography when the key is part of a key pair (public and private key).

If you need to enter keys for symmetric cryptography manually, consider the following recommendations:

- General recommendation:
  Include as much entropy ("randomness") in the key string as possible. A key with a higher entropy is stronger because it is harder to guess by a brute-force attack.
- Detailed recommendations:
  - If possible, let a software tool generate a random value of the required length and in the required format (for example, hexadecimal- or Base64-encoded).
  - If you have to enter a key value manually, avoid including character sequences that repeat, increase or decrease. This lowers the key strength.
    If possible, set up and follow (better: enforce) a policy for manually generated keys.

To help ensure reasonable key strength (see on page 159 “Residual weaknesses of user-generated keys”).

C.1 Quantitative key strength

The strength of a key can be quantified as the number of possible keys for a given key entry scheme. The key entry scheme depends on the key entry policy.

Depending on the actual policy:

- The scheme can be derived from the policy in an optimistic or a skeptic way (see on page 156 “Key entry as ASCII string”).
- The policy strictly specifies a scheme (see on page 157 “Key entry as hexadecimal string”).

C.1.1 Key entry as ASCII string

Let us assume that an example key policy for the entry of a 128-bit key requires an ASCII string of variable length with at least 12 characters, including at least 2 uppercase characters, 2 digits, and 2 special characters.

This is a considerably stronger policy than the password policy assumed in the chapter about high-complexity passwords (see on page 139 “Example (optimistic password strength)”). The reason is that when a manually entered key serves as a master key, its minimum strength should be higher than that of a password.

Note:
To account for the fixed key length, the key value is derived from the variable length ASCII string by a cryptographic hash function, for example, SHA-1. The resulting key has a different value and representation. It may look more random than the original ASCII string, but the derived key has the same strength as the ASCII string.

Example (optimistic key strength)

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use 6 lowercase characters, 2 uppercase characters, 2 digits, and 2 special characters.

Table 32: Key of length 12 ASCII characters, skeptic strength

Character class ID	Class description	Pool characters	Assumed pool size
L	Lowercase characters	a-z	26
U	Uppercase characters	A-Z	26
D	Digits	0-9	10
S	Special characters	!"#$%&()*+’.-/:;	16[1]

1. The special character pool size is given as 16 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The optimistic number of possible keys of this scheme is therefore:

$$N_{pkao} = 26^6 \times 26^2 \times 10^2 \times 16^2 \approx 5.34 \times 10^{15}$$

Where:
- N_{pkao}: Number of possible keys, ASCII entry, optimistic approach

We see that the optimistic number of possible keys enforced by the key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a tiny fraction of about 10^{-23} of the possible keys even in the optimistic view.

Example (skeptic key strength)

We assume a reduced pool size of 8 for each character type to account for frequent characters or digits like "e", "1", or ",".

Table 33: Key of length 12 ASCII characters, skeptic strength

Character class ID	Class description	Pool characters	Assumed, reduced pool size
L	Lowercase characters	a-z	8
U	Uppercase characters	A-Z	8
D	Digits	0-9	8
S	Special characters	!#$&+.-/ (example)	8[1]

1. The special character pool size is given as 8 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The skeptic number of possible keys is therefore:

$$N_{pkas} = 8^6 \times 8^2 \times 8^2 \times 8^2 = 8^{12} = 2^{36} \approx 6.87 \times 10^{10}$$

Where:
- N_{pkas}: Number of possible keys, ASCII entry, skeptic approach

We see that the skeptic number of possible keys enforced by the above key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a minute fraction of about 10^{-28} of the possible keys.

C.1.2 Key entry as hexadecimal string

Example (optimistic policy)

Let us assume that an example key policy for the entry of a 128-bit key requires a hexadecimal string with a length between 16 and 32 characters.

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use just 16 hexadecimal characters.

Table 34: Key of length 16 hex characters, optimistic policy

Character class ID	Class description	Pool characters	Pool size
H	Hexadecimal characters	0-9, a-f	16

The number of possible keys of this scheme is therefore:

$$N_{pkho} = 16^{16} = 2^{64} \approx 1.84 \times 10^{19}$$

Where:
- N_{pkho}: Number of possible keys, hexadecimal characters, optimistic policy

We see that the number of possible keys enforced by the optimistic key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a small fraction of about 10^{-11} of the possible keys even in the optimistic view.

Example (skeptic policy)

The key policy for the entry of a 128-bit key requires a hexadecimal string of fixed length with 32 characters. This is a common situation.

Table 35: Key of length 16 hex characters, skeptic policy

Character class ID	Class description	Pool characters	Pool size
H	Hexadecimal characters	0-9, a-f	16

The number of possible keys of this scheme is therefore:

$N_{pkhs} = 16^{32} = 2^{128} \approx 3.40 \times 10^{38}$

Where:
- N_{pkhs}: Number of possible keys, hexadecimal characters, skeptic policy

We see that the number of possible keys enforced by the skeptic key policy matches the number of theoretically possible different keys. That is, the example key entry policy theoretically enforces a strong key.

Note:
For the entry of a 256-bit key, the policy should require 64 hexadecimal characters. This helps ensure that the number of possible keys for a 256-bit key matches the number of theoretically possible different keys ($2^{256} \approx 1.16 \times 10^{77}$).

C.1.3 Conclusion

As the above examples show, a policy for manual key entry that enforces strong key values shall require a fixed number of hexadecimal characters. The result is a key with a high theoretical strength.

However, the real key strength resulting from a strong policy can still be lower:
- Only truly random key values have the highest possible expected information content.
- Therefore, reasonably strong keys typically shall be generated by an application.
- User-chosen keys typically have significantly less "randomness" (that is, entropy) than application-generated keys and therefore tend to be considerably weaker than application-generated keys, despite matching a strong scheme.

There are two aspects that can impair a key's strength even if it was generated according to a strong scheme:
- Residual weaknesses of user-generated keys
- Residual weaknesses of application-generated keys

Residual weaknesses of user-generated keys

Users, even if following a strong key scheme, might chose hexadecimal keys that include sequences like "1111" or "1234". Even if such a sequence makes up only a part of the key, it impairs the key strength. Reason: Such sequences have a high probability of occurring, which means that their entropy ("randomness") is low. Therefore, such keys are considered weak because these sequences most likely are in an attacker's dictionary. This makes such keys more vulnerable to a dictionary attack, which requires less effort than a brute-force attack.

Even under optimistic assumptions, the probability for a user-generated password to contain an above given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. In reality, the probability is much higher (rough guess: 10^{-3}) because users tend to follow patterns instead of choosing real random sequences. Furthermore, a user-generated key may contain multiple weak sequences which weakens the key further.

Because there are many known weak key sequences, the probability of a user-generated key containing a known weak sequences is rather high – probably too high to be accepted. Therefore, **consider checking a user-chosen key value against a list of known weak sequences.**

Residual weaknesses of application-generated keys

An application-generated key typically is stronger than a user-generated key. Nevertheless, a simple generator for hexadecimal keys might in fact also sometimes suggest keys that include sequences like "1111" or "1234". Such keys may be considered weak because the sequences may be in an attacker's dictionary.

The probability for an application-generated password to contain an above given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. In contrast to user-generated keys, this is a real (skeptic) probability. It is also less likely than for user-generated keys that an application-generated key contains multiple weak sequences.

Because there are many known weak key sequences, the probability of an application-generated key containing one of the known weak sequences may be unacceptable. In this case, **consider checking a system-suggested key value against a list of known weak sequences.**

C.1.4 Example of random key value generation (tool use)

If you have access to a Linux command shell (for example, bash) and have the hexadecimal dump utility `xxd` installed, you can generate a key of reasonable entropy as a hexadecimal string with the following command line:

- For a 256-bit key value (32 bytes):
  $ `xxd -l 32 -c 32 -p /dev/random`
  Example output:
  `26744caec971fc17300df577c8f7e7fda1297aa51881af5be7e58d0de3f55a68`

- For a 128-bit key value (16 bytes):
  $ `xxd -l 16 -c 16 -p /dev/random`
  Example output:
  `d773b4352a6de7c043477b4b55d106ff`

Note:
The random number device `/dev/random` delivers a virtually unlimited sequence of random bytes, with reasonable entropy, in binary format (the byte values are `0x00` .. `0xff`).
You can use other tools than `xxd` to read the desired number of bytes from the random number device and to convert the bytes to the required format.

D Index

A

Abstract of this document . . . 13
Access through OPC UA (setup) . . . 84
Access to the system monitor through the serial port (setup) . . . 94
Acess Control Lists, setup details (network) . . . 119
ACL administration (network) . . . 122
ACL introduction (network) . . . 119
ACL planning (network) . . . 121
ACL setup (network) . . . 121
ACL setup details (network) . . . 119
ACL test (network) . . . 122
ACLs and their associations (network) . . . 121
Advanced user authentication (setup) . . . 95
Advanced user authentication measures (planning) . . . 50
Aggressive assumptions about attackers . . . 136
Alternatives to mitigation (planning) . . . 32
Approximations in this document (Planning) . . . 20
Assess mitigation measure efficiency (planning) . . . 31
Assess the individual threat risks (Planning) . . . 27
Assign IP address parameters to the device management (setup) . . . 78
Assumptions (aggressive) about attackers . . . 136
Assumptions (conservative) about the attack context . . . 137
Assumptions (conservative) about users . . . 136
Attack protection support functions (network) . . . 118
Attack rate mitigation . . . 144
Attack rate mitigation examples . . . 145
Attack resistance time (quantitative) . . . 143
Attack resistance time examples (mitigated attack rate) . . . 145
Attack resistance time examples (unmitigated attack rate) . . . 144
Attack strategies on passwords . . . 135
Audience of this document . . . 13
Audit trail (created by persistent logging) . . . 124
Authentication server considerations (planning) . . . 53

B

Backup of device-specific data (setup) . . . 96
Backup policy for device-related data (planning) . . . 57
Basic security - confidentiality example (Planning) . . . 19
Basic security assumptions for passwords . . . 136
Basics (Planning) . . . 15
Binary or continuous security viewpoints (planning) . . . 35

C

Calculating the required password entropy 148
Capability security levels (introduction) 22
Certificate and revocation management (Planning) 55
Certificates and revocation lists (setup) 91
Checking the security seal (Maintenance) 101
Checking the security seal (Planning) 42
Checking the security seal (setup) 99
Choosing a secure installation location (setup) 69
CLI service shell, disable access (setup) 94
Combining threat risk and mitigation efficiency - criticality (planning) 34, 35
Compilininge a threat profile (Planning) 26
Configuration load priority (Planning) 41
Configuration load priority (Setup) 82
Conservative assumptions about the attack context 137
Conservative assumptions about users 136
Consider data link redundancy requirements (setup) 72
Consider device availability requirements (setup) 69
Consider power budget requirements (setup) 71
Consider power supply redundancy requirements (setup) 70
Considerations for manually generated keys 155
Create backup of device-specific data (setup) 96
Creating ACLs and associations (network) 121
Criticality - Combining threat risk and mitigation efficiency (planning) 34, 35
Criticality assessment and mitigation (Planning) 34

D

Data connections (installation) . . . 99
Data link redundancy requirements (considerations for setup) . . . 72
Decommissioning
Deletion of confidential data and secrets . . . 105
Delivery state, reset to . . . 105
Reset to the delivery state . . . 105
Secure physical destruction of device and possible accessories . . . 106
Decommissioning policy, device hardware (planning) . . . 58
Dedicated HTTPS certificate (setup) . . . 84
Dedicated login banners (setup) . . . 93
Dedicated SNMPv3 authentication and encryption password policy (setup) . . . 89
Dedicated SSH host key pair (setup) . . . 85
Dedicated user account login policy (setup) . . . 86
Dedicated user account password policy (setup) . . . 87
Dedicated user accounts and roles for device management (setup) . . . 88
Defense in depth (network) . . . 108
Defense in depth (system planning) . . . 28
Defense in depth (system planning), responsibilities . . . 29
Defense in depth example (planning) . . . 29
Defense in depth vs. hardening (planning) . . . 28
Defense in depth, detailed example (planning) . . . 30
Deletion of confidential data and secrets (decommissioning) . . . 105
Delivery state (Reset to, decommissioning) . . . 105
Detailed example of defense in depth (planning) . . . 30
Develop the device configuration (setup) . . . 63
Developing a mitigation strategy (planning) . . . 31
Developing a secure boot policy (Planning) . . . 43
Device and port LED visibility (planning) . . . 42
Device and port LEDs (restrict physical (visual) access, Security setup) . . . 98
Device availability (planning) . . . 41
Device decommissioning (overview) . . . 105
Device hardware decommissioning policy (planning) . . . 58
Device hardware interfaces (restrictions to, Security setup) . . . 97
Device hardware repair (maintenance) . . . 103
Device hardware repair policy (planning) . . . 57
Device hardware replacement (maintenance) . . . 102
Device hardware setup (installation) . . . 99
Device hardware, replacement policy (planning) . . . 57
Device installation . . . 99
Device security in the lifecycle phases (main chapter) . . . 63
Device-related data, backup policy (planning) . . . 57
Device-related policies (planning) . . . 57
DHCP server considerations (planning) . . . 52
Disable access (logical) for empty or unused modules (setup) . . . 81
Disable access (logical) to Signal Contact (setup) . . . 80
Disable access (logical) to unused ports and SFP slots (setup) . . . 81
Disable access to the CLI service shell (setup) . . . 94
Disable automatic device software update from external memory (setup) . . . 81
Disable copying a file into the device without valid cryptographic signature (setup) . . . 82
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) (network) . . . 114
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) (network) . . . 110
Disable insecure management protocols (setup) . . . 83
Disable loading configuration profile without valid fingerprint (setup) . . . 83
Disable logical access for empty or unused modules (setup) . . . 81
Disable logical access to Signal Contact (setup) . . . 80
Disable logical access to unused ports and SFP slots (setup) . . . 81
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP (network) . . . 114
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP (network) . . . 110

Disable SNMPv1 traps (setup) 92, 93
Disable writing unencrypted configuration profile to external memory (setup) 83
DNS client functions (setup) 94
DNS server considerations (planning) 53
Document the planned policies 61

E
eMail logging server considerations (Planning) 55
Empty media module slots (restrict physical access) 98
Enable SNMPv3 traps (setup) 93
Entropy (password) 147
Example (Planning) 16
Example of defense in depth (planning) 29
External authentication server considerations (planning) 53
External DHCP server considerations (planning) 52
External DNS server considerations (planning) 53
External log server considerations (planning) 54
External server considerations (planning) 51

G
General vs. security-related device functions (setup) 65

H
Harden your network (network) 108
Hardening vs. defense in depth (planning) 28
Hardware and setup scenarios, relationship 24
Hardware changes (maintenance) 101
Hardware vs. software measures (setup) 64
Help secure the network protocols used (network) 114
Help secure the redundancy protocols used (network) 115
Helping secure the network infrastructure (network) 109
HiDiscovery 77
HiDiscovery (Setup) 78
High-complexity passwords 138
HiView 73
HTTPS certificate (setup) 84

I
Impact of device requirements on system planning 40
Impact of external servers on system planning 51
Impact of network aspects on system planning 51
Impact of system lifecycle on the device lifecycle (planning) 39
Impartial assessment (Planning) 18
Industrial HiVision 11
Installation
  Data connections 99
  Device 99
  Device hardware setup 99
  Signal Contact considerations 99
Intended audience of this document 13
Introduction
  Capability security levels (SL-C) 22
Introduction (network) 107
Introduction (required preparatory work) 22
Introduction to defense in depth (planning) 28
IP access restrictions (setup) 84
IP address parameters for the device management (setup) 78

K

Key rotation 52, 56
Key strength (quantitative) 155
Key strength example (optimistic) 156, 157
Key strength example (skeptic) 157, 158

L

LDAP client (Setup) 95
LDAP server (Planning) 53
LED visibility (device and port LEDs, planning) 42
LEDs (restrict physical (visual) access, Security setup) 98
Lifecycle phases for device security (main chapter) 63
LLDP parameter planning (network) 49
LLDP parameter setup (network) 125
Log server considerations (planning) 54
Logging (setup) 92
Logging parameters (network) 124
Logging policy (planning) 48
Logical vs. physical measures (setup) 64
Login banners (setup) 93
Lookup tables for password policies (quantitative) 150
Low-complexity passwords 140

M

MAC address conflict detection (network) 118
MAC authentication bypass (network) 112
Maintenance
  Checking the security seal 101
  Device hardware replacement 102
  Hardware changes 101
  Hardware repair 103
  Software update 101
Maintenance and operation policy (planning) 60
Maintenance overview (setup) 101
Management IP access restrictions (setup) 84
Management VLAN (setup) 80
Manually generated keys, considerations 155
Measures to help secure the network infrastructure (network) 109
Media module slots (empty, restrict physical access) 98
Mitigation (attack rate) 144
Mitigation efficiency value and unit (planning) 32
Mitigation examples (attack rate) 145
Mitigation strategy development (planning) 31
Mitigation, alternatives (planning) 32

N

Network
Acess Control Lists details (setup) . . . 119
ACL administration . . . 122
ACL introduction . . . 119
ACL planning . . . 121
ACL setup . . . 121
ACL setup details . . . 119
ACL test . . . 122
ACLs and their associations . . . 121
Attack protection support functions . . . 118
Audit trail (created by persistent logging) . . . 124
Creating ACLs and associations . . . 121
Defense in depth . . . 108
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 114
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) . . . 110
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP . . . 114
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP . . . 110
Harden your network . . . 108
Help secure the network protocols used . . . 114
Help secure the redundancy protocols used . . . 115
Helping secure the infrastructure . . . 109
Introduction . . . 107
LLDP parameter planning . . . 49
LLDP parameter setup . . . 125
Logging parameters . . . 124
MAC address conflict detection . . . 118
MAC authentication bypass . . . 112
Measures to help secure the infrastructure . . . 109
Planning the LLDP parameters . . . 49
Port Security . . . 110
Potential conflicts of aims for an ACL . . . 120
Prerequisites . . . 107
Rate limiter . . . 118
Restrict logical access . . . 110
RSTP guards and helper protocols, set up . . . 115
Secure HIPER Ring . . . 117
Secure MRP oder LAG . . . 116
Security support (by the device) . . . 107
Set up DHCP Snooping . . . 111
Set up Dynamic ARP Inspection . . . 112
Set up IP Source Guard . . . 111
Set up RSTP guards and helper protocols . . . 115
Set up Sub Ring with LAG . . . 116
Set up the Denial of Service (DoS) parameters . . . 118
Set up the HIPER Ring parameters . . . 116
Set up the LLDP parameters . . . 125
Set up the logging parameters . . . 124
Set up the Media Redundancy Protocol (MRP) parameters . . . 116
Set up the MRP (Media Redundancy Protocol) parameters . . . 116
Set up the network time synchronization parameters . . . 123
Set up the Redundant Coupling parameters . . . 117
Set up the Ring/Network Coupling parameters . . . 117
Time Synchronization parameters . . . 123
VLAN segregation . . . 110
Network ports or SFP slots (restrict physical access) . . . 98
Network security support (by the device) . . . 107
Network time synchronization considerations (planning) . . . 53

O

Operation and maintenance policy (planning) 60
Operation overview (setup) 100
Overview (Planning) 21
Overview (setup) 76

P

Password and cryptographic key basics (planning) . . . 37
Password attack strategies . . . 135
Password classes . . . 131
Password entropy . . . 147
Password policies . . . 133
Password policy guide . . . 131
Password policy lookup tables (quantitative) . . . 150
Password schemes . . . 134
Password security assumptions . . . 136
Password strength . . . 131
Password strength (quantitative) . . . 138
Password strength example (high-complexity, optimistic) . . . 139
Password strength example (high-complexity, skeptic) . . . 140
Password strength example (low-complexity) . . . 142
Passwords (high-complexity) . . . 138
Passwords (low-complexity) . . . 140
Physical
  Restrict access to empty media module slots (setup) . . . 98
  Restrict access to network ports or SFP slots (setup) . . . 98
  Restrict access to the device and port LEDs (setup) . . . 98
  Restrict access to the Signal Contact (setup) . . . 98
Physical vs. logical measures (setup) . . . 64
Planning
  Advanced user authentication measures . . . 50
  Alternatives to mitigation . . . 32
  Assess mitigation measure efficiency . . . 31
  Assess the individual threat risks . . . 27
  Authentication server considerations . . . 53
  Backup policy for device-related data . . . 57
  Basic mitigation - confidentiality example . . . 19
  Basics . . . 15
  Binary or continuous security viewpoints . . . 35
  Certificate and revocation management . . . 55
  Checking the security seal . . . 42
  Combining threat risk and mitigation efficiency - criticality . . . 34, 35
  Compiling a threat profile . . . 26
  Configuration load priority . . . 41
  Criticality - Combining threat risk and mitigation efficiency . . . 34, 35
  Criticality assessment and mitigation . . . 34
  Decommissioning policy, device hardware . . . 58
  Defense in depth . . . 28
  Defense in depth example . . . 29
  Defense in depth vs. hardening . . . 28
  Defense in depth, detailed example . . . 30
  Defense in depth, introduction . . . 28
  Defense in depth, purpose . . . 28
  Defense in depth, responsibilities . . . 29
  Detailed example of defense in depth . . . 30
  Developing a mitigation strategy . . . 31
  Developing a secure boot policy . . . 43
  Device and port LED visibility . . . 42
  Device availability . . . 41
  Device hardware decommissioning policy . . . 58
  Device hardware repair policy . . . 57
  Device hardware, replacement policy . . . 57
  Device-related data, backup policy . . . 57
  Device-related policies . . . 57
  DHCP server considerations . . . 52

DNS server considerations . . . 53
Document the planned policies . . . 61
eMail logging server considerations . . . 55
Example . . . 16
Example of defense in depth . . . 29
External authentication server considerations . . . 53
External DHCP server considerations . . . 52
External DNS server considerations . . . 53
External log server considerations . . . 54
External server considerations . . . 51
Hardening vs. defense in depth . . . 28
Impact of device requirements on system . . . 40
Impact of external servers on the system . . . 51
Impact of network aspects on the system . . . 51
Impact of system lifecycle on device lifecycle . . . 39
Impartial assessment . . . 18
LDAP server . . . 53
LED visibility (device and port LEDs) . . . 42
Log server considerations . . . 54
Logging policy . . . 48
Maintenance and operation policy . . . 60
Mitigation efficiency value and unit . . . 32
Mitigation strategy development . . . 31
Mitigation, alternatives . . . 32
Network time synchronization considerations . . . 53
Operation and Maintenance policy . . . 60
Overview . . . 21
Password and cryptographic key basics . . . 37
Port and device LED visibility . . . 42
Purpose of . . . 28
RADIUS server . . . 54
Redundancy protocols and VLANs . . . 49
Repair policy, device hardware . . . 57
Replacement policy for device hardware . . . 57
Residual risk . . . 35
Responsibilities for defense in depth . . . 29
Restrictions to the device hardware interfaces . . . 43
Risk value and unit . . . 26
Scenario development . . . 25
Secure installation location . . . 40
Security terminology . . . 15
Security terminology, more . . . 16
Security viewpoints (binary or continuous) . . . 35
Session timeouts . . . 48
Signal contact use . . . 42
Skepticism vs. optimism . . . 18
SNMPv3 authentication and encryption password . . . 47
Software auto update . . . 41
Software update and configuration server considerations . . . 51
SSH key auto upload . . . 41
Strategies to improve security . . . 20
TACACS+ server . . . 54
Tension of convenience vs. security . . . 17
Theoretical and practical degrees of security . . . 20
Threat analysis . . . 19
Unsigned device software, upload . . . 44
Upload of unsigned device software . . . 44
User account and role policy for device management . . . 46
User account login policy . . . 44

User account password policy . . . 45
VLAN . . . 39
VLANs and redundancy protocols . . . 49
Planning for security . . . 15
Planning the LLDP parameters (network) . . . 49
Port and device LED visibility (planning) . . . 42
Port and device LEDs (restrict physical (visual) access, Security setup) . . . 98
Port Security (network) . . . 110
Possible further prerequisites (setup overview) . . . 66
Potential conflicts of aims for an ACL (network) . . . 120
Preparation for installation, suggested (Setup) . . . 67
Preparatory work (introduction) . . . 22
Prerequisites (network) . . . 107
Prerequisites for installation and setup (setup overview) . . . 66
Purpose of defense in depth (planning) . . . 28

Q

Quantitative key strength . . . 155
Quantitative password strength . . . 138

R

RADIUS client (Setup) . . . 95
RADIUS server (Planning) . . . 54
Rate limiter (network) . . . 118
Reasons for suggested installation step sequence (setup) . . . 67
Recommended work step sequence (Setup overview) . . . 67
Redundancy protocols and VLANs (planning) . . . 49
Relationship of hardware and setup scenarios . . . 24
Repair policy, device hardware (planning) . . . 57
Replacement policy for device hardware (planning) . . . 57
Required attack resistance time (quantitative) . . . 146
Required password entropy (calculation) . . . 148
Required preparatory work (introduction) . . . 22
Reset to the delivery state (decommissioning) . . . 105
Residual risk (planning) . . . 35
Responsibilities for defense in depth (system planning) . . . 29
Restrict access to empty media module slots (physical, Security setup) . . . 98
Restrict access to network ports or SFP slots (physical, Security setup) . . . 98
Restrict access to SD card slot (physical, security setup) . . . 97
Restrict access to the device and port LEDs (physical, Security setup) . . . 98
Restrict access to the Signal Contact (physical, Security setup) . . . 98
Restrict access to USB port (physical, security setup) . . . 98
Restrict logical access (network) . . . 110
Restrictions to device hardware interfaces (setup) . . . 97
Restrictions to the device hardware interfaces (planning) . . . 43
Risk value and unit (planning) . . . 26
RSTP guards and helper protocols (network, set up) . . . 115

S

Scenario development (planning) . . . 25
Scenarios (Relationship of hardware and setup scenarios) . . . 24
Scope of this document . . . 21
SD card slot (restrict physical access, Security setup) . . . 97
Secure HIPER Ring (network) . . . 117
Secure installation location (planning) . . . 40
Secure MRP over LAG (network) . . . 116
Secure physical destruction of device and possible accessories (decommissioning) . . . 106
Security assumptions for passwords . . . 136
Security levels (SL-C, introduction) . . . 22
Security planning . . . 15
Security seal . . . 127
Security seal details . . . 127, 128
Security seal overview . . . 127
Security setup overview . . . 76
Security terminology (Planning) . . . 15
Security terminology, more (Planning) . . . 16
Security viewpoints (binary or continuous, planning) . . . 35
Security-related vs. general device functions (setup) . . . 65
Server key rotation . . . 52, 56
Session timeouts (planning) . . . 48
Set up device time synchronization (setup) . . . 90
Set up DHCP Snooping (network) . . . 111
Set up Dynamic ARP Inspection" (network) . . . 112
Set up IP Source Guard (network) . . . 111
Set up RSTP guards and helper protocols (network) . . . 115
Set up Sub Ring with LAG (network) . . . 116
Set up the Denial of Service (DoS) parameters (network) . . . 118
Set up the HIPER Ring parameters (network) . . . 116
Set up the LLDP parameters (network) . . . 125
Set up the logging parameters (network) . . . 124
Set up the MRP (Media Redundancy Protocol) parameters (network) . . . 116
Set up the network time synchronization parameters (network) . . . 123
Set up the Redundant Coupling parameters (network) . . . 117
Set up the Ring/Network Coupling parameters (network) . . . 117
Set up the SSH Known Hosts fingerprints (setup) . . . 86
Set up the the Media Redundancy Protocol (MRP) parameters (network) . . . 116
Set up time synchronization (setup) . . . 90
Setting of secure boot mode (setup) . . . 79
Setup
  Access through OPC UA . . . 84
  Access to the system monitor through the serial port . . . 94
  Advanced user authentication . . . 95
  Assign IP address parameters for the device management . . . 78
  Backup of device-specific data . . . 96
  Certificates and revocation lists . . . 91
  Checking the security seal . . . 99
  Choosing a secure installation location . . . 69
  CLI service shell, disable access . . . 94
  Configuration load priority . . . 82
  Consider data link redundancy requirements . . . 72
  Consider device availability requirements . . . 69
  Consider power budget requirements . . . 71
  Consider power supply redundancy requirements . . . 70
  Create backup of device-specific data . . . 96
  Data link redundancy requirements . . . 72
  Dedicated HTTPS certificate . . . 84
  Dedicated login banners . . . 93

Dedicated SNMPv3 authentication and encryption password policy . . . 89
Dedicated SSH host key pair . . . 85
Dedicated user account login policy . . . 86
Dedicated user account password policy . . . 87
Dedicated user accounts and roles for device management . . . 88
Develop the device configuration . . . 63
Device hardware . . . 99
Device hardware interfaces (restrictions to) . . . 97
Device time synchronization . . . 90
Disable access (logical) for empty or unused modules . . . 81
Disable access (logical) to Signal Contact . . . 80
Disable access (logical) to unused ports and SFP slots . . . 81
Disable access to the CLI service shell . . . 94
Disable automatic device software update from external memory . . . 81
Disable copying a file into the device without valid cryptographic signature . . . 82
Disable insecure management protocols . . . 83
Disable loading configuration profile without valid fingerprint . . . 83
Disable logical access for empty or unused modules . . . 81
Disable logical access to Signal Contact . . . 80
Disable logical access to unused ports and SFP slots . . . 81
Disable SNMPv1 traps . . . 92, 93
Disable writing unencrypted configuration profile to external memory . . . 83
DNS client functions . . . 94
Enable SNMPv3 traps . . . 93
General vs. security-related device functions . . . 65
Hardware vs. software measures . . . 64
HiDiscovery . . . 78
HTTPS certificate . . . 84
IP access restrictions . . . 84
IP address parameters for the device management . . . 78
LDAP client . . . 95
Logging . . . 92
Logical vs. physical measures . . . 64
Login banners . . . 93
Maintenance overview . . . 101
Management IP access restrictions . . . 84
Management VLAN . . . 80
Operation overview . . . 100
Physical vs. logical measures . . . 64
Preparation for installation, suggested . . . 67
Prerequisites for installation and setup . . . 66
RADIUS client . . . 95
Reasons for suggested installation step sequence . . . 67
Restrict access to SD card slot (physical) . . . 97
Restrict physical access to USB port . . . 98
Restrictions to device hardware interfaces . . . 97
SD card slot (restrict physical access, Security setup) . . . 97
Security-related vs. general device functions . . . 65
Set up the SSH Known Hosts fingerprints . . . 86
Setting of secure boot mode . . . 79
SNMPv1 traps . . . 92, 93
SNMPv3 authentication and encryption password policy . . . 89
SNMPv3 traps . . . 93
Software update . . . 73
Software vs. hardware measures . . . 64
Specify finite session timeouts . . . 90
SSH host key pair . . . 85
SSH key auto upload . . . 81
Suggested installation step sequence (reasons for) . . . 67

Suggested preparation for installation . . . 67
System monitor, Access through the serial port . . . 94
TACACS+ client . . . 95
Time synchronization . . . 90
USB port (restrict physical access) . . . 98
User account login policy . . . 86
User account password policy . . . 87
User accounts and roles for device management . . . 88
VLAN dedicated to management access . . . 80
Setup overview . . . 76
Setup overview (Possible further prerequisites) . . . 66
SFP slots or network ports (restrict physical access) . . . 98
Signal Contact (restrict physical access, Security setup) . . . 98
Signal Contact considerations (installation) . . . 99
Signal contact use (planning) . . . 42
Skepticism (Basic approximations) . . . 20
Skepticism (Planning) . . . 20
Skepticism vs. optimism (Planning) . . . 18
SL-C (introduction) . . . 22
SNMPv1 traps (setup) . . . 92, 93
SNMPv3 authentication and encryption password (planning) . . . 47
SNMPv3 authentication and encryption password policy (setup) . . . 89
SNMPv3 traps (setup) . . . 93
Software auto update (Planning) . . . 41
Software update (maintenance) . . . 101
Software update (setup) . . . 73
Software update and configuration server considerations (Planning) . . . 51
Software vs. hardware measures (setup) . . . 64
Specify finite session timeouts (setup) . . . 90
SSH host key pair (setup) . . . 85
SSH key auto upload (Planning) . . . 41
SSH key auto upload (Setup) . . . 81
SSH server key rotation . . . 52, 56
Strategies to improve security (Planning) . . . 20
Subject of this document . . . 21
Suggested installation step sequence (reasons for, setup) . . . 67
Suggested preparation for installation (Setup) . . . 67
Summary of this document . . . 13
Synopsis of this document . . . 13
System monitor, Access through the serial port (setup) . . . 94

T

TACACS+ client (Setup) . . . 95
TACACS+ server (Planning) . . . 54
Technical Documents . . . 175
Technical questions . . . 175
Technical Support . . . 175
Tension of convenience vs. security (Planning) . . . 17
Theoretical and practical degrees of security (Planning) . . . 20
Threat analysis (Planning) . . . 19
Time Synchronization parameters (network) . . . 123
Training courses . . . 175

U

Unsigned device software, upload (Planning) 44
Upload of unsigned device software (Planning) 44
USB port (restrict physical access, security setup) 98
User account and role policy for device management (planning) 46
User account login policy (planning) 44
User account login policy (setup) 86
User account password policy (planning) 45
User account password policy (setup) 87
User accounts and roles for device management (setup) 88

V

VLAN (planning) 39
VLAN dedicated to management access (setup) 80
VLAN segregation (network) 110
VLANs and redundancy protocols (planning) 49

W

Work step sequence (recommended, Setup overview) 67

E Technical 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.belden.com.

For technical support, visit my.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/services/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.

F 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:

	Very Good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND