HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

BXS HiOS-2S Rel. 10.6.00



Reference Manual

Graphical User Interface

User Manual

Configuration

Security

HIRSCHMANN
A BELDEN BRAND

Reference Manual

Graphical User Interface
BOBCAT IP30/40 Extended Switch
HiOS-2S

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 . . . 7

About this Manual . . . 9

Key . . . 10

Notes on the Graphical User Interface . . . 11
Language Toggle . . . 11
Banner . . . 12
Menu pane . . . 13
Dialog area . . . 15

1 Basic Settings . . . 19
1.1 System . . . 19
1.2 Network . . . 23
1.2.1 Global . . . 24
1.2.2 IPv4 . . . 26
1.2.3 IPv6 . . . 30
1.3 Out-of-Band over USB . . . 34
1.4 Software . . . 36
1.5 Load/Save . . . 40
1.6 External Memory . . . 53
1.7 Port . . . 56
1.8 Power over Ethernet . . . 62
1.8.1 PoE Global . . . 64
1.8.2 PoE Port . . . 67
1.9 Restart . . . 70

2 Time . . . 73
2.1 Basic Settings . . . 73
2.2 SNTP . . . 77
2.2.1 SNTP Client . . . 78
2.2.2 SNTP Server . . . 82
2.3 PTP . . . 84
2.3.1 PTP Global . . . 85
2.3.2 PTP Boundary Clock . . . 87
2.3.2.1 PTP Boundary Clock Global . . . 88
2.3.2.2 PTP Boundary Clock Port . . . 93
2.3.3 PTP Transparent Clock . . . 96
2.3.3.1 PTP Transparent Clock Global . . . 97
2.3.3.2 PTP Transparent Clock Port . . . 100
2.4 802.1AS . . . 101
2.4.1 802.1AS Global . . . 102
2.4.2 802.1AS Port . . . 106
2.4.3 802.1AS Statistics . . . 115

3	**Device Security**	117
3.1	User Management	117
3.2	Authentication List	127
3.3	Management Access	130
3.3.1	Server	131
3.3.2	IP Access Restriction	145
3.3.3	Web	149
3.3.4	Command Line Interface	150
3.3.5	SNMPv1/v2 Community	152
3.4	Pre-login Banner	153
3.5	SSH Known Hosts	154
4	**Network Security**	157
4.1	Network Security Overview	157
4.2	Port Security	158
4.3	802.1X	163
4.3.1	802.1X Global	164
4.3.2	802.1X Port Configuration	166
4.3.3	802.1X Port Clients	172
4.3.4	802.1X EAPOL Port Statistics	174
4.3.5	802.1X Port Authentication History	176
4.3.6	802.1X Integrated Authentication Server (IAS)	178
4.4	RADIUS	180
4.4.1	RADIUS Global	182
4.4.2	RADIUS Authentication Server	184
4.4.3	RADIUS Accounting Server	188
4.4.4	RADIUS Authentication Statistics	190
4.4.5	RADIUS Accounting Statistics	192
4.5	DoS	193
4.5.1	DoS Global	194
4.6	ACL	197
4.6.1	ACL IPv4 Rule	198
4.6.2	ACL MAC Rule	202
4.6.3	ACL Assignment	205
5	**Switching**	209
5.1	Switching Global	209
5.2	Rate Limiter	211
5.3	Filter for MAC Addresses	214
5.4	IGMP Snooping	216
5.4.1	IGMP Snooping Global	218
5.4.2	IGMP Snooping Configuration	220
5.4.3	IGMP Snooping Enhancements	224
5.4.4	IGMP Snooping Querier	227
5.4.5	IGMP Snooping Multicasts	230
5.5	Time-Sensitive Networking	231
5.5.1	TSN Configuration	232
5.5.2	TSN Gate Control List	235

5.5.2.1 TSN Configured Gate Control List . . . 236
5.5.2.2 TSN Current Gate Control List . . . 239
5.6 MRP-IEEE . . . 240
5.6.1 MRP-IEEE Configuration . . . 241
5.6.2 MRP-IEEE Multiple MAC Registration Protocol . . . 242
5.6.3 MRP-IEEE Multiple VLAN Registration Protocol . . . 247
5.7 GARP . . . 250
5.7.1 GMRP . . . 251
5.7.2 GVRP . . . 253
5.8 QoS/Priority . . . 254
5.8.1 QoS/Priority Global . . . 255
5.8.2 QoS/Priority Port Configuration . . . 256
5.8.3 802.1D/p Mapping . . . 258
5.8.4 IP DSCP Mapping . . . 260
5.8.5 Queue Management . . . 262
5.9 VLAN . . . 263
5.9.1 VLAN Global . . . 265
5.9.2 VLAN Configuration . . . 266
5.9.3 VLAN Port . . . 268
5.9.4 VLAN Voice . . . 270
5.10 L2-Redundancy . . . 272
5.10.1 MRP . . . 273
5.10.2 HIPER Ring . . . 277
5.10.3 Spanning Tree . . . 278
5.10.3.1 Spanning Tree Global . . . 279
5.10.3.2 Spanning Tree Port . . . 285
5.10.4 Link Aggregation . . . 292
5.10.5 Link Backup . . . 299

6 Diagnostics . . . 303
6.1 Status Configuration . . . 303
6.1.1 Device Status . . . 304
6.1.2 Security Status . . . 308
6.1.3 MAC Notification . . . 316
6.1.4 Alarms (Traps) . . . 317
6.1.4.1 Trap V3 User Management . . . 318
6.1.4.2 Trap Destinations . . . 322
6.2 System . . . 324
6.2.1 System Information . . . 325
6.2.2 Hardware State . . . 326
6.2.3 Configuration Check . . . 327
6.2.4 IP Address Conflict Detection . . . 329
6.2.5 ARP . . . 333
6.2.6 Selftest . . . 335
6.3 Syslog . . . 337
6.4 Ports . . . 340
6.4.1 TP cable diagnosis . . . 341

6.4.2 Port Monitor . . . 343
6.4.3 Auto-Disable . . . 353
6.4.4 Port Mirroring . . . 357
6.5 LLDP . . . 359
6.5.1 LLDP Configuration . . . 360
6.5.2 LLDP Topology Discovery . . . 364
6.6 Report . . . 368
6.6.1 Report Global . . . 369
6.6.2 Persistent Logging . . . 373
6.6.3 System Log . . . 376
6.6.4 Audit Trail . . . 377

7 Advanced . . . 379
7.1 DHCP . . . 379
7.1.1 DHCP Server . . . 379
7.1.1.1 DHCP Server Global . . . 380
7.1.1.2 DHCP Server Pool . . . 382
7.1.1.3 DHCP Server Lease Table . . . 389
7.2 DHCP L2 Relay . . . 390
7.2.1 DHCP L2 Relay Configuration . . . 391
7.2.2 DHCP L2 Relay Statistics . . . 394
7.3 Industrial Protocols . . . 395
7.3.1 IEC 61850/MMS . . . 396
7.3.2 Modbus TCP . . . 399
7.3.3 EtherNet/IP . . . 401
7.3.4 PROFINET . . . 403
7.4 Command Line Interface . . . 407

A Index . . . 409

B Technical support . . . 415

C Readers' Comments . . . 416

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 16.



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
- Network
- Out-of-Band over USB
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet
- 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.

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*
- *IEC 61850/MMS*
- *PROFINET*

Note:
Specify a device name that is compatible with PROFINET: max. 240 characters, not starting with a number. The participants in the network read the device name using SNMP and PROFINET DCP.

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 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.

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.

Dashed border

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

1.2 Network

[Basic Settings > Network]

The menu contains the following dialogs:
- Global
- IPv4
- IPv6

1.2.1 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.

1.2.2 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.

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

Netmask

Specifies the netmask.

Possible values:

- Valid IPv4 netmask

Gateway address

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

Possible values:

- Valid IPv4 address

BOOTP/DHCP

Client ID

Displays the DHCP client ID that the device sends to the BOOTP or DHCP server. If the server is 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.

1.2.3 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 16.

Prefix

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

PrefixLength

Displays the prefix length of the IPv6 address.

Unlike an IPv4 address, 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.

1.3 Out-of-Band over USB

[Basic Settings > Out-of-Band over USB]

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

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

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

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

Operation

Operation

Enables/disables the USB network interface.

Possible values:

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

Management interface

Device MAC address

Displays the MAC address of the USB network interface.

Host MAC address

Displays the MAC address of the connected management station.

IP parameter

Verify that the IP subnet of this network interface 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 USB network interface.

Possible values:

- Valid IPv4 address
  (default setting: `192.168.248.100`)
  The device assigns this IP address, increased by 1, to the management station that is connected to the device.
  Example: `192.168.248.100` for the USB network interface, `192.168.248.101` for the management station.

Netmask

Specifies the netmask.

Possible values:

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

1.4 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 10.3.03.
  - 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 16.

Buttons

Update Firmware

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

- 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
- *usb*
  External USB memory (ACA22-USB-C (EEC))

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.

1.5 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 16.

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 external memory (*ENVM*).

☐ 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 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

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

Possible values:

- *usb*
  External USB memory (ACA22-USB-C (EEC))

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.

Configuration encryption

Active

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

Possible values:

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

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

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

Set password

Opens the *Set password* window that helps you to enter the password needed for the configuration profile encryption. Encrypting the configuration profiles makes unauthorized access more difficult. To do this, perform the following steps:

- 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*).

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

1.6 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 16.

Type

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

Possible values:

- *usb*
  External USB memory (ACA22-USB-C (EEC))

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*
  The device loads the configuration profile from the external memory (*ENVM*).
  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* 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.

1.7 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 16.

Port

Displays the port number.

Name

Name of the port.

Possible values:

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

Port on

Activates/deactivates the port.

Possible values:

- `marked` (default setting)
  The port is active.
- `unmarked`
  The port is inactive. The port does not send or receive any data.

State

Displays if the port is currently physically enabled or disabled.

Possible values:

- `marked`
  The port is physically enabled.
- `unmarked`
  The port is physically disabled.
  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)
  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
  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 HDX`
  Half-duplex connection
- `10M FDX`
  Full-duplex connection
- `100M HDX`
  Half-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection

Note:
The operating modes of the port actually available depend on the device hardware.

Link/Current settings

Displays the operating mode which the port currently uses.

Possible values:

- `-`
  No cable connected, no link.
- `10M HDX`
  Half-duplex connection
- `10M FDX`
  Full-duplex connection
- `100M HDX`
  Half-duplex connection
- `100M FDX`
  Full-duplex connection
- `1G FDX`
  Full-duplex connection

Note:
The operating modes of the port actually available depend on the device hardware.

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) or collisions (half-duplex operation) is activated on the port.
  - ☐ To enable the flow control in the device, also activate the *Flow control* function in the *Switching > Global* dialog.
  - ☐ Activate the flow control also on the port of the device that is connected to this port.

  On an uplink port, activating the flow control can possibly cause undesired sending 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..9720` (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.

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 16.

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.

1.8 Power over Ethernet

[Basic Settings > Power over Ethernet]

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

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

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

You manage the power output with the *Priority* parameter. When the sum of the power required by the connected devices exceeds the power available, the device turns off the power supplied to the ports according to the set-up priority. The device turns off the power supplied to the ports, starting with the ports set-up as low priority. When several ports have the same priority, the device turns off power, starting with the highest-numbered ports.

The menu contains the following dialogs:

- PoE Global
- PoE Port

1.8.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

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

Operation

Operation

Enables/disables the *Power over Ethernet* function.

Possible values:

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

Configuration

Send trap

Activates/deactivates the sending of SNMP traps. If the power consumption exceeds the user-specified threshold value, then the device sends an SNMP trap.

Possible values:

- `marked` (default setting)
  The device sends SNMP traps. 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 device does not send any SNMP traps.

Threshold [%]

Specifies the threshold value for the power consumption in percent.

If the power output exceeds this threshold value, then the device measures the total output power and sends an SNMP trap.

Possible values:

- `0..99` (default setting: `90`)

System power

Max. Budget [W]

Displays the maximum available global power budget.

Reserved [W]

Displays the global reserved power. The device reserves power according to the detected classes of connected powered devices. Reserved power is equal to or less than the actual delivered power.

Delivered [W]

Displays the actual power delivered to the modules in watts.

Delivered [mA]

Displays the actual current delivered to the modules in milliamperes.

Table

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

Module

Device module to which the table rows relate.

Configured power budget [W]

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

Possible values:

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

Max. power budget [W]

Displays the maximum power available for this module.

Reserved power [W]

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

Delivered power [W]

Displays the actual power in watts delivered to powered devices connected to this port.

Delivered current [mA]

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

Power source

Displays the power sourcing equipment for the device.

Possible values:

- *internal*
  Internal power source
- *external*
  External power source

Threshold [%]

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

Possible values:

- `0..99` (default setting: `90`)

Send trap

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

Possible values:

- `marked` (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 power consumption of the module exceeds the user-defined threshold value, then the device sends an SNMP trap.
- `unmarked`
  The sending of SNMP traps is inactive.

1.8.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

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

Table

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

Port

Displays the port number.

PoE enable

Activates/deactivates the PoE power provided to the port.

When the device activates or deactivates the function, the device logs an event in the System Log).

Possible values:

- `marked` (default setting)
  Providing PoE power to the port is active.
- `unmarked`
  Providing PoE power to the port is inactive.

Fast startup

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

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

Possible values:

- `marked`
  The fast start up function is active. The device sends power to the powered devices (PD) immediately after turning the power to the device on.
- `unmarked` (default setting)
  The fast start up function is inactive. The device sends power to the powered devices (PD) after loading its own configuration.

Priority

Specifies the *Port priority*.

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

Possible values:

- *critical*
- *high*
- *low* (default setting)

Status

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

Possible values:

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

Detected class

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

Possible values:

- *class0*
- *class1*
- *class2*
- *class3*
- *class4*

class0
class1
class2
class3
class4

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

Possible values:

- marked (default setting)
- unmarked

Consumption [W]

Displays the current power consumption of the port in watts.

Possible values:

- `0..30`

Consumption [mA]

Displays the current delivered to the port in milliamperes.

Possible values:

- `0..600`

Power limit [W]

Specifies the maximum power in watts that the port outputs.

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

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

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

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

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

Possible values:

- `0..30` (default setting: `0`)
  You can specify the value in steps of 0.1 W.

Max. consumption [W]

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

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

Name

Specifies the name of the port.

Specify the name of your choice.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters

Auto-shutdown power

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

Possible values:

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

Disable power at [hh:mm]

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

Possible values:

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

Re-enable power at [hh:mm]

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

Possible values:

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

1.9 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 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.

2 Time

The menu contains the following dialogs:
- Basic Settings
- SNTP
- PTP
- 802.1AS

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 11.

[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 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

2.2.1 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 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Index

Displays the index number to which the table row relates.

The device automatically assigns the value when you add a table row. When you delete a table row, this leaves a gap in the numbering. When you 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

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.

2.2.2 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.

2.3 PTP

[Time > PTP]

The menu contains the following dialogs:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.3.1 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.

In the device, either the *802.1AS* function or the *PTP* function can be enabled at the same time.

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`

2.3.2 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

2.3.2.1 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.

2.3.2.2 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 16.

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.

2.3.3 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

2.3.3.1 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.

2.3.3.2 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 16.

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.

2.4 802.1AS

[Time > 802.1AS]

The IEEE 802.1AS-2020 protocol describes a method that enables precise synchronization of the clocks of time-aware devices in the network. When you use the protocol 802.1AS over the Ethernet, you can think of the protocol as a profile of IEEE 1588-2019.

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.

The *802.1AS* function has the following specifications:
- In the device, either the *802.1AS* function or the *PTP* function can be enabled.
- If the *SNTP* function and the *802.1AS* function are enabled in the device at the same time, then the *802.1AS* function has priority.
- The *802.1AS* function supports 2 PTP instances, each associated with a *domain ID*.

The menu contains the following dialogs:
- 802.1AS Global
- 802.1AS Port
- 802.1AS Statistics

2.4.1 802.1AS Global

[Time > 802.1AS > Global]

In this dialog, you specify basic settings for the *802.1AS* function.

Operation

Operation

Enables/disables the *802.1AS* function.

Possible values:

- *On*
  The *802.1AS* function is enabled.
  The device synchronizes its clock using the *802.1AS* function.
  Consider activating the *802.1AS* function for each instance and also on the individual ports.

- *Off* (default setting)
  The *802.1AS* function is disabled.
  When disabling the *802.1AS* function globally, you disable time synchronization for both instances and for the respective ports allocated to them. This disables time synchronization on the instance and port levels even if the *802.1AS* function is enabled on the instances and on the individual ports.

Configuration

Sync lower bound [ns]

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

Possible values:

- `0..999999999 (10⁹-1)` (default setting: `30`)

Sync upper bound [ns]

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

Possible values:

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

Status

This frame displays the synchronization settings of the device for *Instance 0*.

Offset to master [ns]

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

Steps removed

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

When the device operates in the *Slave* role, the value `1` means that the device is connected with the reference time source (*Grandmaster*) directly through one communication path.

Clock identity

Displays the clock identification number of the device.

The device displays the identification number as a byte sequence in hexadecimal notation.

The device identification number consists of the MAC address of the device followed by:

- `00:01` for *Instance 0*
- `00:02` for *Instance 1*

Max. offset absolute [ns]

Displays the maximum measured time difference in nanoseconds that has occurred since the device synchronized its local clock with the reference time source (*Grandmaster*).

Is synchronized

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

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

You specify the synchronization threshold values in the *Configuration* frame.

Grandmaster

This frame displays the criteria that the *Best Master Clock* algorithm uses when determining the reference time source (*Grandmaster*) for *Instance 0*.

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.

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 *Time > 802.1AS > Global* 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*). This is a parameter used by the *Best Master Clock* algorithm.

Clock accuracy

Displays the estimated accuracy of the reference time source (*Grandmaster*). This is a parameter used by the *Best Master Clock* algorithm.

Clock variance

Displays the variance of the reference time source (*Grandmaster*), also known as the *Offset scaled log variance*. This is a parameter used by the *Best Master Clock* algorithm.

Priority 2

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

Clock identity

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

The device identification number consists of the MAC address of the device followed by:

- `00:01` for *Instance 0*
- `00:02` for *Instance 1*

Parent

This frame displays the settings of the directly superior master device for *Instance 0*.

Clock identity

Displays the port identification number of the directly superior master device.

The device identification number consists of the MAC address of the device followed by:

- `00:01` for *Instance 0*
- `00:02` for *Instance 1*

Port

Displays the port number of the directly superior master device.

Cumulative rate ratio [ppm]

Displays the measured frequency difference of the local clock in ppm (parts per million) relative to the reference time source (*Grandmaster*).

2.4.2 802.1AS Port

[Time > 802.1AS > Port]

In this dialog, you specify the *802.1AS* settings for each instance and on each individual port.

[Instance]

The device can be part of multiple *PTP domains*. In the device, the *802.1AS* function supports 2 instances: *Instance 0* and *Instance 1*, each operating within separate *PTP domains*.

You set up each instance separately:
- *Instance 0*
  for synchronizing device clocks and transmitting time synchronization messages
- *Instance 1*
  only for transmitting time synchronization messages

Operation

Operation

Enables/disables the *802.1AS* function for the respective instance.

Possible values:

▶ *On*
The *802.1AS* function is enabled.
The device synchronizes its local clock using the *802.1AS* function.
Consider activating the *802.1AS* function on the individual ports.

▶ *Off* (default setting)
The *802.1AS* function is disabled.

Configuration

Priority 1

Specifies the *priority 1* value for the instance.

Possible values:

▶ `0..255` (default setting: `248`)
Verify that you use the value `255` for a *PTP instance* that is not Grandmaster-capable.

Priority 2

Specifies the *priority 2* value for the instance.

Possible values:

▶ `0..255` (default setting: `247`)
Verify that you use the value `255` for a *PTP instance* that is not Grandmaster-capable.

Domain number

Specifies the domain number.

If a port is part of the same domain for both *Instance 0* and *Instance 1*, then the dialog displays an error message.

Possible values:

- `0..127` (default settings: `0` for *Instance 0* and `1` for *Instance 1*)

External port configuration

Activates/deactivates the manual setup of the port roles.

Possible values:

- `marked`
  Manual setup is active.
  You can select the desired port roles from the *Desired Role* drop-down list.
- `unmarked` (default setting)
  Manual setup is inactive.
  The device auto-negotiates port roles.

Table

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

Port

Displays the port number.

Active

Activates/deactivates the *802.1AS* function on the port.

Possible values:

- `marked` (default setting)
  The *802.1AS* function is active on the port.
  On the port, the device synchronizes its clock using the *802.1AS* function.
  The prerequisite is that none of the following protocols are active on the port:
  – *Link Aggregation*
- `unmarked`
  The *802.1AS* function is inactive on the port.

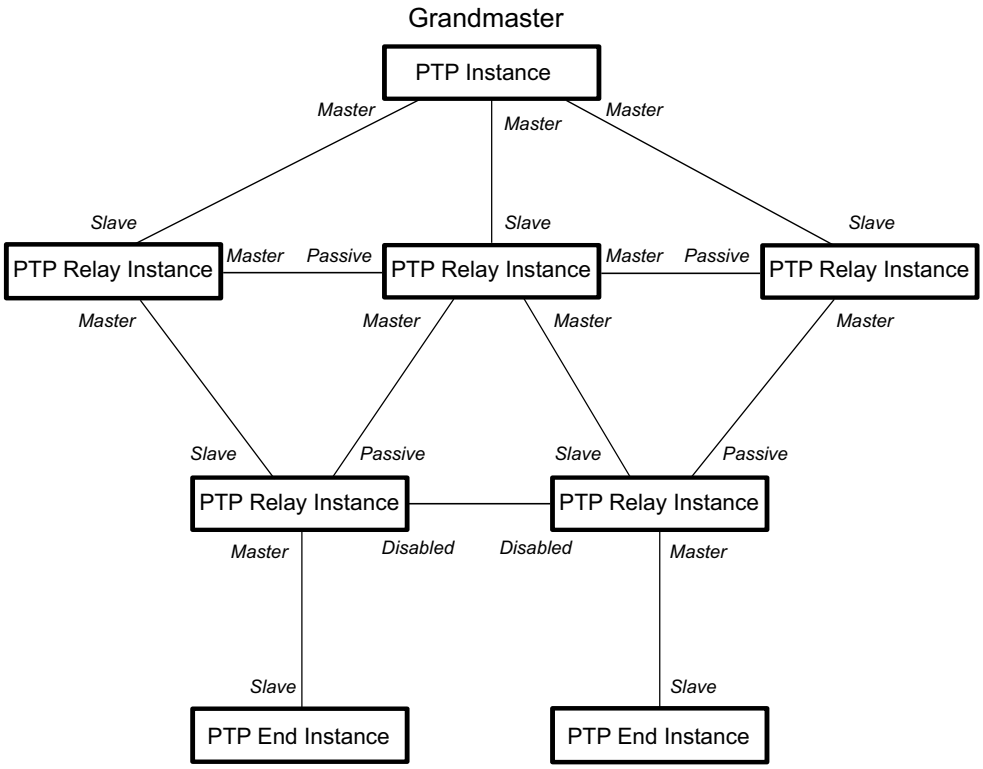
Role

Displays the current role that the port operates in within the *802.1AS* domain.

Possible values:

- *Disabled*
  The port is not *802.1AS*-capable.
- *Master*
  The port operates in the *Master* role.

- *Passive*
  The port operates in the *Passive* role.
- *Slave*
  The port operates in the *Slave* role.



Inspired by: IEEE Std 802.1AS-2020

Desired Role

Specifies the desired role for the port. If the checkbox in the *External port configuration* column is marked, then auto-negotiation of port roles is disabled. You can then manually set the desired port role.

Possible values:

- *Disabled*
  The port is not *802.1AS*-capable.
- *Master*
  The port operates in the *Master* role.
- *Passive*
  The port operates in the *Passive* role.
- *Slave*
  The port operates in the *Slave* role.

AS capable

Displays if the port of the device and the port of the neighboring device are both *802.1AS*-capable and have the *802.1AS* function enabled.

Possible values:

- `marked`
  The connected ports are *802.1AS*-capable and have the *802.1AS* function enabled.
  The prerequisites are:
  - The checkbox in the *Measuring delay* column is marked. The device measures the delay (*Peer delay*) on the port.
  - The value you specify in the *Peer delay threshold [ns]* column is higher than the value in the *Peer delay [ns]* column.
- `unmarked` (default setting)
  At least one of the connected ports is not *802.1AS*-capable or does not have the *802.1AS* function enabled.

Initial announce interval [s]

Specifies the interval in seconds at which the port, in the `Master` role, sends *Announce* messages for *802.1AS* topology discovery.

Possible values:

- `1..2` (default setting: `1`)
  Assign the same value to every device of an *802.1AS* domain.
- `-`
  The port does not send *Announce* messages.

Settable announce interval [s]

Specifies the interval in seconds at which the port, in the `Master` role, sends *Announce* messages for *802.1AS* topology discovery.

If the checkbox in the *Use settable announce interval* column is marked, then the device uses this value instead of the value specified in the *Initial announce interval [s]* column. During the first synchronization, the device uses the value in the *Initial announce interval [s]* column even if the *Use settable announce interval* checkbox is marked.

Possible values:

- `1..2` (default setting: `1`)
  Assign the same value to every device of an *802.1AS* domain.
- `-`
  The port does not transmit *Announce* messages.

Use settable announce interval

Activates/deactivates the use of the interval specified in the *Settable announce interval [s]* column for sending *Announce* messages. The device sends *Announce* messages for *802.1AS* topology discovery.

Possible values:

- `marked` (default setting)
  The device sends *Announce* messages in the interval specified in the *Settable announce interval [s]* column.
- `unmarked`
  The device sends *Announce* messages in the interval specified in the *Initial announce interval [s]* column.

Announce timeout

Specifies the number of *Announce* intervals that the device waits for to receive an *Announce* message on this port from the neighboring port.

Example: In the default setting, where *Settable announce interval [s]* = `1` and *Announce timeout* = `3`, the total timeout in seconds is 1 s × 3 = 3 s.

When the specified interval elapses without receiving an *Announce* message, the device tries to find a new path to the reference time source (*Grandmaster*) using the *Best Master Clock* algorithm. If the device finds a reference time source (*Grandmaster*), then it assigns the `Slave` role to the port through which the new path leads. If the device does not find a reference time source (*Grandmaster*), the device itself becomes the reference time source (*Grandmaster*) and assigns the `Master` role to its ports.

Possible values:

- `2..10` (default setting: `3`)
  Assign the same value to each port that belongs to the same *802.1AS* domain.

Initial sync interval [s]

Specifies the interval in seconds at which the port, in the `Master` role, sends *Sync* messages for time synchronization.

Possible values:

- `0.125` (default setting)
- `0.250`
- `0.5`
- `1`
- `-`
  The port does not send *Sync* messages.

Settable sync interval [s]

Specifies the interval in seconds at which the port, in the `Master` role, sends *Sync* messages for time synchronization.

If the checkbox in the *Use settable sync interval* column is marked, then the device uses this value instead of the value specified in the *Initial sync interval [s]* column. During the first synchronization, the device uses the value in the *Initial sync interval [s]* column even if the *Use settable sync interval* checkbox is marked.

Possible values:

- `0.125` (default setting)
- `0.250`
- `0.5`
- `1`
- `-`
  The port does not send *Sync* messages.

Use settable sync interval

Activates/deactivates the use of the value in the *Settable sync interval [s]* column for sending *Sync* messages.

Possible values:

- `marked` (default setting)
  The device sends *Sync* messages in the interval specified in the *Settable sync interval [s]* column.
- `unmarked`
  The device sends *Sync* messages in the interval specified in the *Initial sync interval [s]* column.

Sync timeout

Specifies the number of *Sync* intervals the device waits for to receive a *Sync* message on this port from the neighboring port.

Example: In the default setting, where*Settable sync interval [s]* = `0.125` and*Sync timeout* = `3`, the total timeout in seconds is 0.125 s × 3 = 0.375 s.

When the number of intervals elapses without receiving a *Sync* message, the device tries to find a new path to the reference time source using the *Best Master Clock* algorithm. If the device finds a reference time source (*Grandmaster*), then it assigns the *`Slave`* role to the port through which the new path leads. Otherwise, the device itself becomes the reference time source (*Grandmaster*) and assigns the *`Master`* role to its ports.

Possible values:

- `2..10` (default setting: `3`)
  Assign the same value to each port that belongs to the same *802.1AS* domain.

Initial pdelay interval [s]

Specifies the interval in seconds at which the port sends a *Peer delay request* message to the neighboring port to measure the *Peer delay*.

Possible values:

- `1` (default setting)
- `2`
- `4`
- `8`
- `-`
  The port does not send *Peer delay request* messages.

Settable pdelay interval [s]

Specifies the interval in seconds at which the port sends a *Peer delay request* message to the neighboring port to measure the *Peer delay*.

If the checkbox in the *Use settable pdelay interval* column is marked, then the devices uses this value instead of the value specified in the *Initial pdelay interval [s]* column. During the first synchronization, the device uses the value in the *Initial pdelay interval [s]* column even if the *Use settable pdelay interval* checkbox is marked.

Possible values:

- `1` (default setting)
- `2`
- `4`

- 8
- –
  The port does not send *Peer delay request* messages.

Use settable pdelay interval

Activates/deactivates the use of the value in the *Settable pdelay interval [s]* column for sending *Peer delay request* messages.

Possible values:

- marked
  The device sends *Peer delay request* messages in the interval specified in the *Settable pdelay interval [s]* column.
- unmarked (default setting)
  The device sends *Peer delay request* messages in the interval specified in the *Initial pdelay interval [s]* column.

Initial GptpCapable interval [s]

Specifies the interval in seconds at which the port sends a message to the neighboring port about the device capability for time synchronization.

Possible values:

- 1 (default setting)
- 2
- 4
- 8
- –
  The port does not send *gPTP-capable* messages.

Settable GptpCapable interval [s]

Specifies the interval in seconds at which the port sends a message to the neighboring port about the device capability for time synchronization.

If the checkbox in the*Use settable GptpCapable interval* column is marked, the device uses this value instead of the value specified in the *Initial GptpCapable interval [s]* column. During the first synchronization, the device uses the value in the *Initial GptpCapable interval [s]* column even if the *Use settable GptpCapable interval* checkbox is marked.

Possible values:

- 1 (default setting)
- 2
- 4
- 8
- –
  The port does not send *gPTP-capable* messages.

Use settable GptpCapable interval

Activates/deactivates the use of the value in the *Settable GptpCapable interval [s]* column for sending messages that contain *gPTP-capable* information.

Possible values:

- `marked`
  The device sends *gPTP-capable* messages in the interval specified in the *Settable GptpCapable interval [s]* column.
- `unmarked` (default setting)
  The device sends *gPTP-capable* messages in the interval specified in the *Initial GptpCapable interval [s]* column.

GptpCapable timeout

Specifies the number of *gPTP-capable* intervals that the device waits for to receive a *gPTP-capable* message on this port from the neighboring port.

When the number of intervals elapses without receiving a *gPTP-capable* message, the device assigns the `Disabled` role to the port. The port is no longer *gPTP-capable*.

Possible values:

- `1..255` (default setting: `9`)

Peer delay timeout

Specifies the number of *Peer delay* intervals that the device waits for to receive a *Peer delay* message from the neighboring port.

When the number of intervals elapses without receiving a *Peer delay* message, the device assigns the `Disabled` role to the port. The port is no longer *802.1AS*-capable. See the *AS capable* column.

Possible values:

- `1..255` (default setting: `9`)

Allowed faults

Specifies the number of detected faults above which the device no longer considers the port as *802.1AS*-capable. The device assigns the `Disabled` role to the port.

Examples of such detected faults are:

- The *Peer delay threshold [ns]* value exceeds the upper threshold.
- The calculated *Neighbor rate ratio [ppm]* is invalid.

Possible values:

- `1..255` (default setting: `9`)

Peer delay threshold [ns]

Specifies the upper threshold value for the *Peer delay* in nanoseconds. If the value in the *Peer delay [ns]* column is greater than this value, then the device assigns the *Disabled* role to the port. The port is no longer *802.1AS*-capable. See the *AS capable* column.

Possible values:

- `0..1000000 (10⁶)` (default setting: `10000`)

Measuring delay

Displays if the device measures the delay (*Peer delay*) on the port.

Possible values:

- `marked`
  The device measures the delay (*Peer delay*) on the port. You find the measured value in the *Peer delay [ns]* column.
- `unmarked`
  The device does not measure the delay (*Peer delay*) on the port.

Peer delay [ns]

Displays the *Peer delay* value in nanoseconds the device measured. The prerequisite is that the checkbox in the *Measuring delay* column is marked.

Asymmetry

Specifies the time difference in nanoseconds between the mean link delay value (*Peer delay [ns]* / 2) and the propagation time from the port to its neighbor.

Possible values:

- `-10000000000..10000000000 (10¹⁰)` (default setting: `0`)

Neighbor rate ratio [ppm]

Displays the measured frequency difference of the local clock in parts per million relative to the clock in the adjacent device.

2.4.3 802.1AS Statistics

[Time > 802.1AS > Statistics]

This dialog displays information about the number of messages received, sent, or discarded on the ports. The dialog also displays counters that increment every time a timeout event occurred.

[Instance]

The device displays information for each instance separately.

Table

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

Port

Displays the port number.

Sync timeout

Displays the number of times that a *Sync timeout* event occurred on the port. See the *Sync timeout* column in the *Time > 802.1AS > Port* dialog.

Announce timeout

Displays the number of times that the *Announce timeout* event occurred on this port. See the *Announce timeout* column in the *Time > 802.1AS > Port* dialog.

Delay timeout

Displays the number of times that the *Peer delay timeout* event occurred on this port. See the *Peer delay timeout* column in the *Time > 802.1AS > Port* dialog.

Received messages

Displays the counters for messages received on the ports.

Sync

Displays the number of *Sync* messages.

Sync follow-up

Displays the number of *Sync follow-up* messages.

Delay request

Displays the number of *Peer delay request* messages.

Delay response

Displays the number of *Peer delay response* messages.

Delay response follow-up

Displays the number of *Peer delay response follow-up* messages.

Announce

Displays the number of *Announce* messages.

Discarded

Displays the number of *Sync* messages that the device discarded on this port. The device discards a *Sync* message for example, in cases where the port does not receive a *Sync follow-up* message for a corresponding *Sync* message.

Transmitted messages

Displays the counters for messages transmitted on the ports:

Sync

Displays the number of *Sync* messages.

Sync follow-up

Displays the number of *Sync follow-up* messages.

Delay request

Displays the number of *Peer delay request* messages.

Delay response

Displays the number of *Peer delay response* messages.

Delay response follow-up

Displays the number of *Peer delay response follow-up* messages.

Announce

Displays the number of *Announce* messages.

3 Device Security

The menu contains the following dialogs:
- User Management
- Authentication List
- 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 16.

Buttons


Add

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

- In the *User name* field, you specify the name of the user account.
  Possible values:
  - Alphanumeric ASCII character string with 1..32 characters


Remove

Removes the selected table row.

User name

Displays the name of the user account.

To 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 123.

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 123.

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 123.

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 123.

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
- RADIUS

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

In the default setting the following authentication lists are available:
- `defaultDot1x8021AuthList`
- `defaultLoginAuthList`
- `defaultV24AuthList`

Table

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

Note:
If the table does not contain a list, then 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* 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 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.

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 Management Access

[Device Security > Management Access]

The menu contains the following dialogs:

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

3.3.1 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 16.

SNMPv1

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SNMPv2

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SNMPv3

Displays if the server service is active or inactive, which authorizes access to the device using SNMP version 3. See the *SNMP* tab.

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

Telnet server

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

Possible values:

- `marked`
  Server service is active.
- `unmarked`
  Server service is inactive.

SSH server

Displays if the server service is active or inactive, which authorizes access to the device using Secure Shell (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.
- `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.
- `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.

3.3.2 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 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Index

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

When you delete a table row, this leaves a gap in the numbering. When you 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.

IEC 61850/MMS

Activates/deactivates the access to the MMS server.

Possible values:

- `marked` (default setting)
  IEC 61850/MMS access is active. Access is possible from the adjacent IP address range.
- `unmarked`
  IEC 61850/MMS access is inactive.

Modbus TCP

Activates/deactivates the access to the *Modbus TCP* server.

Possible values:

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

EtherNet/IP

Activates/deactivates the access to the *EtherNet/IP* server.

Possible values:

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

PROFINET

Activates/deactivates the access to the *PROFINET* server.

Possible values:

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

3.3.3 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.

3.3.4 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 USB-C 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: `(BXS)`

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>`

3.3.5 SNMPv1/v2 Community

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

In this dialog, you specify the community name for SNMPv1/v2 applications.

Applications send requests using SNMPv1/v2 with a community name in the SNMP data packet header. Depending on the community name (see *Community* 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 16.

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.
- `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)

3.4 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>`

3.5 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 16.

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
- 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 16.

Buttons


Wizard

Opens the *Wizard* window that helps you associate the ports with the address of one or more desired senders. See “[Wizard: Port security]” on page 161.

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.

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.

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.

Table

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

Port

Displays the port number.

Port 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.

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.

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`.

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`

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.

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`)

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*.

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*.

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 16.

Port

Displays the port number.

User name

Displays the user name with which the end device logged in.

MAC address

Displays the MAC address of the end device.

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.

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* 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 16.

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 16.

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 16.

Buttons

Add

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

- In the *User name* field, you specify the name of the user account on the end device.

Remove

Removes the selected table row.

User name

Displays the name of the user account on the end device.

To 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 179.

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 16.

Buttons


Add

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

- In the *Index* field, you specify the index number.
- In the *Address* field, you specify the IP address of the server.
- 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 186.

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 16.

Buttons


Add

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

- In the *Index* field, you specify the index number.
- In the *Address* field, you specify the IP address of the server.
- 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 186.

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 16.

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 16.

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.

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 IP Broadcast Pings. Broadcast Pings are a known evidence for Smurf Attacks.

Possible values:

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

Information

Packets dropped

Displays the number of data packets that the device has discarded.

4.6 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.
- *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 rule and specify the rule settings. See the *Network Security > ACL > IPv4 Rule* dialog, or the *Network Security > ACL > MAC Rule* dialog.
- ☐ Assign the Access Control List to the ports and VLANs of the device. See the *Network Security > ACL > Assignment* dialog.

The menu contains the following dialogs:

- ACL IPv4 Rule
- ACL MAC Rule
- ACL Assignment

4.6.1 ACL IPv4 Rule

[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

Table

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

Buttons

 Add

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

- 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*
  - *Packet fragmented*

Source IP address

Specifies the source address of the IP data packets to which the device applies the rule.

Possible values:

- `?.?.?.?` (default setting)
  The device applies the rule to IP data packets with any source address.
- Valid IPv4 address
  The device applies the rule to IP data packets with the specified source address.
  You use the `?` character as a wild card.
  Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`.
- Valid IPv4 address/bit mask
  The device applies the rule to IP data packets with the specified source address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example `192.168.1.0/0.0.0.127`: The device applies the rule to IP data packets with a source address in the range from `192.168.1.0` to `….127`.

Destination IP address

Specifies the destination address of the IP data packets to which the device applies the rule.

Possible values:

- `?.?.?.?` (default setting)
  The device applies the rule to IP data packets with any destination address.
- Valid IPv4 address
  The device applies the rule to data packets with the specified destination address.
  You use the `?` character as a wild card.
  Example `192.?.?.32`: The device applies the rule to IP data packets whose source address begins with `192.` and ends with `.32`.
- Valid IPv4 address/bit mask
  The device applies the rule to data packets with the specified destination address. The inverse bit mask lets you specify the address range with bit-level accuracy.
  Example `192.168.1.0/0.0.0.127`: The device applies the rule to IP data packets with a destination address in the range from `192.168.1.0` to `….127`.

Protocol

Specifies the IP protocol or Layer 4 protocol type of the data packets to which the device applies the rule. The device applies the rule only to data packets 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.

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.

Action

Specifies how the device processes received IP data packets when the device applies the rule.

Possible values:

- *`permit`* (default setting)
  The device forwards the IP data packets.
- *`deny`*
  The device drops the IP data packets.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- `marked`
  Logging is active.
  The prerequisite is that in the *Network Security > ACL > Assignment* dialog the Access Control List is assigned to a VLAN or port.
  The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to IP data packets.
- `unmarked` (default setting)
  Logging is inactive.

The device lets you activate this function for up to 128 deny rules.

4.6.2 ACL MAC Rule

[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

Table

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

Buttons

 Add

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

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`.

Action

Specifies how the device processes received MAC data packets when the device applies the rule.

Possible values:

- *permit* (default setting)
  The device forwards the MAC data packets.
- *deny*
  The device discards the MAC data packets.

Log

Activates/deactivates the logging in the log file. See the *Diagnostics > Report > System Log* dialog.

Possible values:

- marked
  Logging is active.
  The prerequisite is that in the *Network Security > ACL > Assignment* dialog the Access Control List is assigned to a VLAN or port.
  The device registers in the log file, in an interval of 30 s, how many times it applied the deny rule to MAC data packets.
- unmarked (default setting)
  Logging is inactive.

The device lets you activate this function for up to 128 deny rules.

4.6.3 ACL Assignment

[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 50 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*).

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.

Table

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

Buttons


Add

Opens the *Create* window to assign a rule to a port or a VLAN.
- 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 that the device applies the Access Control List to received data packets. The device can apply the Access Control Lists only to received data packets.

Priority

Displays the priority of the Access Control List.

Using the priority, you specify the sequence in which the device applies the Access Control Lists to the data stream. The device applies the rules in ascending order which starts with priority 1. If an Access Control List is assigned to a port and to a VLAN with the same priority, then the device applies the rules to the port first.

Possible values:

- `1..4294967295 (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
- Time-Sensitive Networking
- 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

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.
- In half-duplex mode, the device simulates a collision.

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.

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.

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 16.

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.

Known multicast mode

Activates/deactivates the rate limiter function for received known 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.

Known 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 frame mode

Activates/deactivates the rate limiter function for received unicast and multicast 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.

Unknown frame 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 16.

Port

Displays the port number.

Bandwidth [%]

Specifies the egress transmission rate.

Possible values:

- `0` (default setting)
  The bandwidth limitation is disabled.
- `1..100`
  The bandwidth limitation is enabled.
  This value specifies the percentage of overall link speed for the port in 1% increments.

5.3 Filter for MAC Addresses

[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 16.

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 16.

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`)

Unknown multicasts

Specifies how the device forwards data packets with unknown Multicast addresses. The prerequisite is that in the *Switching > IGMP Snooping > Multicasts* dialog, *Configuration* frame, *Unknown multicasts* option list, the *flood* radio button is selected.

Possible values:

- *discard*
  The device discards data packets with an unknown MAC Multicast address.
- *flood*
  The device forwards data packets with an unknown MAC Multicast address to every port.
- *query ports*
  The device forwards data packets with an unknown MAC Multicast address to the query ports. You can assign this item to a maximum of 16 VLANs in this dialog.

[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 16.

Port

Displays the port number.

Active

Activates/deactivates the *IGMP Snooping* function on the port.

The prerequisite is that the *IGMP Snooping* function is globally enabled.

Possible values:

- `marked` (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.
- `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 16.

Buttons

Wizard

Opens the *Wizard* window that helps you select and set up the ports. See “[Wizard: IGMP snooping enhancements]” on page 225.

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 16.

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.
  You can overwrite this setting per VLAN. See the *Unknown multicasts* column in the *Switching* > IGMP Snooping > *Configuration* dialog, *VLAN ID* tab.

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 16.

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 Time-Sensitive Networking

[Switching > TSN]

The menu contains the following dialogs:

- TSN Configuration
- TSN Gate Control List

5.5.1 TSN Configuration

[Switching > TSN > Configuration]

In this dialog, you enable the *TSN* function and specify the time-specific settings.

The device supports time-aware queuing defined in IEEE 802.1Qbv. This *TSN* feature lets the TSN-capable ports transmit data packets of every *traffic class* scheduled relative to a defined cycle in the Gate Control List. The VLAN tag of an Ethernet packet – or the *Port priority* in case of an untagged packet – contains the priority.

The feature helps to avoid latency and congestion loss for reserved data streams. The precise synchronization of cycles and gate states using the Precision Time Protocol (PTP) according to IEEE 1588 makes congestion-free, low-latency communication possible. The prerequisite is that every device in the network supports IEEE 802.1Qbv.

Note:

In contrast to the Command Line Interface, you commit the settings immediately if you click the button.

Operation

Operation

Enables/disables the *TSN* function in the device.

Possible values:

- *On*
  The *TSN* function is globally enabled.
  The device processes link-local frames on the TSN-capable ports with the priority of *traffic class* `6`. As a result, the link-local frames compete with other data packets with the same or higher priority when forwarding. This affects the following frame types:
  - RSTP
  - LLDP
  - IEEE 802.1AS
  - PTP Peer Delay
- *Off* (default setting)
  The *TSN* function is globally disabled.
  As long as the *TSN* function is active on a port, the port uses the opened gates `0,1,2,3,4,5,6,7`.
  This setting is preset by the manufacturer.

Base time

Date
Time
[ns]

Specifies the time at which the cycle starts related to the Universal Time Coordinated (UTC).

The device converts the value into the PTP time scale directly without considering the leap seconds.

Possible values:

- `<Day of the week, date>`
  (depending on the language and region settings of your computer)
- `hh:mm:ss AM/PM`
  Hour:Minute:Second
- `0..999999999 (10⁹-1)`
  Specifies the offset of nanoseconds.

Note:
When you specify the base time in the future, the cycle starts as many seconds earlier than specified in the *UTC offset [s]* field. See the *Time > PTP > Boundary Clock > Global* dialog.

Configuration

Cycle time [ns]

Specifies the duration of a cycle in nanoseconds.

Possible values:

- `50000..10000000 (10⁷)` (default setting: `1000000`)
  50 µs .. 10 ms

Table

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

On devices with 16 or more ports, the *TSN* function is available on the following ports:
- `1/1..1/8` on a device with 16 ports
- `1/1..1/12` on a device with 20 or 24 ports

Port

Displays the port number.

Active

Activates/deactivates the *TSN* function on the port.

Possible values:

- `marked`
  The *TSN* function is active on the port.
  When you specify the base time in the future, the cycle starts at the time specified in the *Base time* frame.
  The prerequisite is that the *PTP* function is enabled and the device is synchronized.
  As long as the *TSN* function is globally enabled, the port uses the cycle specified in the *Switching > TSN > Gate Control List > Configured* dialog.
- `unmarked` (default setting)
  The *TSN* function is inactive on the port.
  As long as the *TSN* function is globally enabled, the port uses the opened gates `0,1,2,3,4,5,6,7`.

Port state

Displays the status of the cycle on the port.

Possible values:

- *running*
  The cycle is running.
  The port uses the cycle specified in the *Switching > TSN > Gate Control List > Configured* dialog.
- *waitForTimeSync*
  The cycle has not yet started.
  The clock of the device is not synchronized.
  Check the *PTP* settings.
- *pending*
  The cycle has not yet started.
  The base time is specified in the future.
- *disabled*
  The cycle is not running.
  The *TSN* function is inactive on the port.
  - Check the setting in the *Operation* frame.
  - Check the setting in the *Active* column.

  The port uses the gate states specified in the *Default gate states* column.
- *error*
  The cycle is not running.
  An error was detected.

Time of last activation

Displays the date and time at which the time settings became active last time.

This value relates to the PTP time.

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

The menu contains the following dialogs:

- TSN Configured Gate Control List
- TSN Current Gate Control List

5.5.2.1 TSN Configured Gate Control List

[Switching > TSN > Gate Control List > Configured]

In this dialog, you specify the time slots of the cycle for the TSN-capable ports. Adding a table row you specify the opened gates and the duration of the time slot.

Note:

In contrast to the Command Line Interface, you commit the settings immediately if you click the button.

The dialog contains the following tabs:

- One tab for every TSN-capable port.
  The number of TSN-capable ports depends on the device.

[<Port number>]

Configuration

Status

Displays the template assigned to the Gate Control List.

Possible values:

- `-`
  No template. No entries are assigned to the Gate Control List.
- *`default 2 time slots`*
  Template with 3 entries:
  - First entry is the *traffic class* `7`.
  - Second entry is the *traffic class* `6` to `0`.
  - Third entry is a guard band.
- *`default 3 time slots`*
  Template with 5 entries:
  - First entry is the *traffic class* `7`.
  - Second entry is a guard band.
  - Third entry is the *traffic class* `6`.
  - Fourth entry is the *traffic class* `5` to `0`.
  - Fifth entry is a guard band.
- <`any other template name`>
  The template was assigned using the Command Line Interface.

Template

Opens the *Template* window to assign a different template to the Gate Control List. When you select a different template and click the *Ok* button, the device replaces the entries in the table.

From the drop-down list, you select one of the following templates:

- *default 2 time slots*
- *default 3 time slots*

The device lets you assign additional templates using the Command Line Interface.

Table

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

Buttons

Delete

Deletes the selected table row.

Index

Displays the index number of the entry in the Gate Control List, which specifies the chronological order of the timeslots.

Gate states

Specifies the opened gates in case the *TSN* function on the port is active.

- The data packets whose *traffic class* is assigned to a selected gate are selected for transmission – Gate state *OPEN*.
- The data packets whose *traffic class* is assigned to a not selected gate are not selected for transmission – Gate state *CLOSED*.

Possible values:

- `-` (default setting)
  No gate selected.
  The device does not open any gate on the port during the time slot is processed. From the drop-down list, unselect every gate.
- `0..7`
  The device opens the selected gates on the port during the time slot is processed. From the drop-down list, select one or more items.
  You assign the VLAN priorities to a *traffic class* in the *Switching > QoS/Priority > 802.1D/p Mapping* dialog.

Interval [ns]

Specifies the duration of the time slot in nanoseconds.

Possible values:

▶ `1000..10000000 (10⁷)`

When you specify the duration of the time slots, consider the following conditions:

- A single time slot
  - Confirm that a time slot is at least long enough for the port to transmit the longest expected data packet.
  - Confirm that a time slot is less than or equal to the duration of the cycle.
- The sum of the time slots specified
  - We recommend that the sum of the time slots is equal to the duration of the cycle.
  - If the sum exceeds the duration of the cycle, then the overlapping time slots are discarded and the cycle restarts.
  - If the sum is smaller than the duration of the cycle, then the interval of the last time slot is extended to fit into the cycle.

Note:
Discrepancies between the specified time slots and the cycle duration are not highlighted in the *Switching > TSN > Gate Control List > Current* dialog.

5.5.2.2 TSN Current Gate Control List

[Switching > TSN > Gate Control List > Current]

In this dialog, you monitor the current settings of the cycle for the TSN-capable ports. Every table row represents a specified time slot.

If the time at which the cycle starts (*Base time*) is in the future, then the displayed values are different from the values specified in the *Switching > TSN > Gate Control List > Configured* dialog.

In the *Switching > TSN > Configuration* dialog, the *Port state* column displays if the cycle is running on a port.

The dialog contains the following tabs:
- One tab for every TSN-capable port.
  The number of TSN-capable ports depends on the device.

[<Port number>]

Table

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

Index

Displays the index number of the entry in the Gate Control List, which specifies the chronological order of the timeslots.

Gate states

Displays the opened gates in case the *TSN* function on the port is active.

Interval [ns]

Displays the duration of the time slot in nanoseconds.

5.6 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

5.6.1 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 16.

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`)

5.6.2 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 16.

Port

Displays the port number.

Active

Activates/deactivates the port MMRP participation.

Possible values:

- `marked` (default setting)
  With MMRP enabled globally and on this port, the device sends and receives MMRP messages on this port.
- `unmarked`
  Disables the port MMRP participation.

Restricted group registration

Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

Possible values:

- `marked`
  If enabled and a static filter entry for the MAC address exists on the VLAN concerned, then the device registers the MAC address attributes dynamically.
- `unmarked` (default setting)
  Activates/deactivates the restriction of dynamic MAC address registration using MMRP on the port.

[Service requirement]

This tab contains forwarding parameters for each active VLAN, specifying the ports on which multicast forwarding applies. The device lets you statically setup VLAN ports as *Forward all* or Forbidden. You set the Forbidden MMRP service requirement statically only through the Graphical User Interface or Command Line Interface.

A port is setup only as ForwardAll or Forbidden.

Table

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

VLAN ID

Displays the ID of the VLAN.

<Port number>

Specifies the service requirement handling for the port.

Possible values:

- FA
  Specifies the ForwardAll traffic setting on the port. The device forwards the data packets destined to MMRP registered multicast MAC addresses on the VLAN. The device forwards the data packets to ports which MMRP has dynamically setup or ports which the administrator has statically setup as ForwardAll ports.
- F
  Specifies the Forbidden traffic setting on the port. The device blocks dynamic MMRP ForwardAll service requirements. With ForwardAll requests blocked on this port in this VLAN, the device blocks the data packets destined to MMRP registered multicast MAC addresses on this port. Furthermore, the device blocks MMRP service request for changing this value on this port.
- - (default setting)
  Disables the forwarding functions on this port.
- Learned
  Displays values setup by MMRP service requests.

[Statistics]

Devices on a LAN exchange Multiple MAC Registration Protocol Data Units (MMRPDUs) to maintain statuses of devices on an active MMRP port. This tab lets you monitor the MMRP data packets statistics for each port.

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 16.

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.

5.6.3 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 16.

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 16.

Port

Displays the port number.

Transmitted MVRP PDU

Displays the number of MVRPDUs transmitted on the port.

Received MVRP PDU

Displays the number of MVRPDUs received on the port.

Received bad header PDU

Displays the number of MVRPDUs with a bad header that the device received on the port.

Received bad format PDU

Displays the number of MVRPDUs with a bad data field that the device blocked on the port.

Transmission failed

Displays the number of MVRPDUs that the device blocked on the port.

Registrations failed

Displays the number of unsuccessful registration attempts on the port.

Last received MAC address

Displays the MAC address from which the port last received MVRPDUs.

5.7 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

5.7.1 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 16.

Port

Displays the port number.

GMRP active

Activates/deactivates the port *GMRP* participation.

The prerequisite is that the *GMRP* function is globally enabled.

Possible values:

- `marked` (default setting)
  The port *GMRP* participation is active.
- `unmarked`
  The port *GMRP* participation is inactive.

Service requirement

Specifies the ports on which multicast forwarding applies.

Possible values:

- *`Forward all unregistered groups`* (default setting)
  The device forwards data destined to *GMRP*-registered multicast MAC addresses on the VLAN.
  The device forwards data to the unregistered groups.
- *`Forward all groups`*
  The device forwards data destined to every group, registered or unregistered.

5.7.2 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 16.

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.

5.8 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

5.8.1 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).

5.8.2 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 16.

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`

5.8.3 802.1D/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 16.

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

5.8.4 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 16.

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

5.8.5 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 16.

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.

5.9 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
- Port-based VLAN

The menu contains the following dialogs:
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice

5.9.1 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.

5.9.2 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.

Table

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

Buttons


Add

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

In the *VLAN ID* field, you specify the VLAN ID.


Remove

Removes the selected table row.

VLAN ID

ID of the VLAN.

The device supports up to 128 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

<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.

5.9.3 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 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.

Table

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

Port

Displays the port number.

Port-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.

5.9.4 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 16.

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`

5.10 L2-Redundancy

[Switching > L2-Redundancy]

The menu contains the following dialogs:

- MRP
- HIPER Ring
- Spanning Tree
- Link Aggregation
- Link Backup

5.10.1 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.

This value is relevant in the context of the *PROFINET* function. See the *Advanced > Industrial Protocols > PROFINET* dialog.

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.

5.10.2 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.

5.10.3 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 menu contains the following dialogs:

- Spanning Tree Global
- Spanning Tree Port

5.10.3.1 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

Displays the protocol used for the *Spanning Tree* function:

Possible values:

- *rstp*
  The protocol RSTP is active.
  With RSTP (IEEE 802.1Q-2005), the *Spanning Tree* function operates for the underlying physical layer.

Traps

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.

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`)

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>`

5.10.3.2 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]

[CIST]

In this tab you have the option to activate the Spanning Tree function on the ports individually, specify the settings for *Edge ports*, and view the current values. The abbreviation CIST stands for *Common and Internal Spanning Tree*.

Note:
Deactivate the *Spanning Tree* function on the ports that are participating in other Layer 2 redundancy protocols. Otherwise, it is possible that the redundancy protocols operate differently than intended. This can cause loops.

Table

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

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.
- *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* 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 half-duplex link or through a hub.

Port BPDU filter

Activates/deactivates the filtering of STP-BPDUs on the port explicitly.

The prerequisite is that the port is a manually specified *Edge port*. For these ports, the checkbox in the *Admin edge port* column is marked.

Possible values:

- `marked`
  The BPDU filter is active on the port.
  The function excludes the port from *Spanning Tree* operations.
  - The device does not send STP-BPDUs on the port.
  - The device drops any STP-BPDUs received on the port.
- `unmarked` (default setting)
  The BPDU filter is inactive on the port.
  You have the option to globally activate the BPDU filter for every *Edge port*. See the *Switching* > L2-Redundancy > *Spanning Tree* > *Global* dialog, *Bridge configuration* frame.
  If the *BPDU filter (all admin edge ports)* checkbox is marked, then the BPDU filter is still active on the port.

BPDU filter status

Displays if the BPDU filter is active on the port.

Possible values:

- `marked`
  The BPDU filter is active on the port as a result of the following settings:
  - The checkbox in the *Port BPDU filter* column is marked.
    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 16.

Port

Displays the port number.

Root guard

Activates/deactivates the monitoring of STP-BPDUs on the port. The prerequisite is that the *Loop guard* function is inactive.

With this setting the device helps you protect 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.

5.10.4 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 2 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 16.

Buttons

 Add

Opens the *Create* window to add a table row for a LAG interface or to assign a physical port to a LAG interface.

- From the *Trunk port* drop-down list, you select the LAG interface number.
- From the *Port* drop-down list, you select the number of a physical port to assign to the LAG interface.

After you 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*
  - *802.1AS*
- 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.

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..9720` (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)

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* 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.

5.10.5 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 16.

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Primary port

Displays the *Primary port* of the interface pair. When you enable the Link Backup function, this port is responsible for forwarding the data packets.

Possible values:

- Physical ports

Backup port

Displays the *Backup port* 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*.

6 Diagnostics

The menu contains the following dialogs:

- Status Configuration
- System
- Syslog
- Ports
- LLDP
- Report

6.1 Status Configuration

[Diagnostics > Status Configuration]

The menu contains the following dialogs:

- Device Status
- Security Status
- 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 16.

Connection errors

Activates/deactivates the monitoring of the link status of the port/interface.

Possible values:

- `marked`
  Monitoring is active.
  If the link interrupts on a monitored port/interface, then in the *Device status* frame, the value changes to `error`.
  In the *Port* tab, you have the option of selecting the ports/interfaces to be monitored individually.
- `unmarked` (default setting)
  Monitoring is inactive.

Temperature

Activates/deactivates the monitoring of the temperature in the device.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the temperature exceeds 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.

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.

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.

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.

[Port]

Table

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

Port

Displays the port number.

Propagate connection error

Activates/deactivates the monitoring of the link on the port/interface.

Possible values:

- `marked`
  Monitoring is active.
  If the link on the selected port/interface is interrupted, then in the *Device status* frame, the value changes to *error*.
- `unmarked` (default setting)
  Monitoring is inactive.

This setting takes effect when you mark the *Connection errors* checkbox in the *Global* tab.

[Status]

Table

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

Timestamp

Displays the date and time of the event.

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 16.

Password default settings unchanged

Activates/deactivates the monitoring of the password for the locally set up user account `admin`.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If the password is set to the default setting for the `admin` user account, then in the *Security status* frame, the value changes to *`error`*.
- `unmarked`
  Monitoring is inactive.

You set the password in the *Device Security > User Management* dialog.

Min. password length 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`.
- `unmarked`
  Monitoring is inactive.

IEC 61850/MMS active

Activates/deactivates the monitoring of the *IEC 61850/MMS* function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the *IEC 61850/MMS* function, then in the *Security status* frame, the value changes to *error*.
- `unmarked`
  Monitoring is inactive.

You enable/disable the *IEC 61850/MMS* function in the *Advanced > Industrial Protocols > IEC 61850/MMS* dialog, *Operation* frame.

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.

Modbus TCP active

Activates/deactivates the monitoring of the *Modbus TCP* function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the *Modbus TCP* function, then in the *Security status* frame, the value changes to *error*.
- `unmarked`
  Monitoring is inactive.

You enable/disable the *Modbus TCP* function in the *Advanced > Industrial Protocols > Modbus TCP* dialog, *Operation* frame.

EtherNet/IP active

Activates/deactivates the monitoring of the *EtherNet/IP* function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the *EtherNet/IP* function, then in the *Security status* frame, the value changes to *error*.
- `unmarked`
  Monitoring is inactive.

You enable/disable the *EtherNet/IP* function in the *Advanced > Industrial Protocols > EtherNet/IP* dialog, *Operation* frame.

PROFINET active

Activates/deactivates the monitoring of the *PROFINET* function.

Possible values:

- `marked` (default setting)
  Monitoring is active.
  If you enable the *PROFINET* function, then in the *Security status* frame, the value changes to `error`.
- `unmarked`
  Monitoring is inactive.

You enable/disable the *PROFINET* function in the *Advanced > Industrial Protocols > PROFINET* dialog, *Operation* frame.

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 16.

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 16.

Timestamp

Displays the date and time of the event.

Cause

Displays the event which caused the SNMP trap.

6.1.3 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 16.

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.

6.1.4 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

6.1.4.1 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 16.

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 320.

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 320.

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.

6.1.4.2 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 16.

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 16.

Flash region

Displays the name of the parameter, for example for the relevant memory area.

Description

Displays a description for the parameter.

Flash sectors

Displays how many sectors are assigned to the memory area.

Sector erase operations

Displays how many times the device has overwritten the sectors of the memory area.

6.2.3 Configuration Check

[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 16.



Displays detailed information about the detected deviations in the area below the table row. To hide the detailed information again, click the  button. If you click the icon in the table header, you display or hide the detailed information for each table row.

ID

Displays the rule ID of the deviations having occurred. The dialog combines several deviations with the same rule ID under one rule ID.

Level

Displays the level of deviation between the settings in this device and the settings in the detected neighboring devices.

The device differentiates between the following access statuses:

- *Information*
  The performance of the communication between the two devices is not impaired.
- *Warning*
  The performance of the communication between the two devices is possibly impaired.
- *Error*
  The communication between the two devices is impaired.

Message

Displays a summary of the detected deviations.

6.2.4 IP Address Conflict Detection

[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 16.

Timestamp

Displays the time at which the device detected an address conflict.

Port

Displays the number of the port on which the device detected the address conflict.

IP address

Displays the IP address that is causing the address conflict.

MAC address

Displays the MAC address of the device with which the address conflict exists.

6.2.5 ARP

[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 16.

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, set the device to the Recovery Mode.

▶ `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 16.

Cause

Detected error causes to which the device reacts.

Possible values:

- *task*
  The device detects errors in the applications executed, for example if a task terminates or is not available.
- *resource*
  The device detects errors in the resources available, for example if the memory is becoming scarce.
- *software*
  The device detects software errors, for example error in the consistency check.
- *hardware*
  The device detects hardware errors, for example in the chip set.

Action

Specifies how the device behaves if the adjacent event occurs.

Possible values:

- *logOnly*
  The device registers the detected error in the log file. See the *Diagnostics > Report > System Log* dialog.
- *sendTrap*
  The device sends an SNMP trap.
  The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.
- *reboot* (default setting)
  The device triggers a restart.

6.3 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.

Table

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

Buttons

Add

Adds a table row.

Remove

Removes the selected table row.

Index

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

When you delete a table row, this leaves a gap in the numbering. When you 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

Destination UDP port

Specifies the UDP port on which the syslog server expects the log entries.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `514`)

Transport type

Displays the transport type the device uses to send the events to the syslog server.

Possible values:

- *udp*
  The device sends the events over the UDP 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.

6.4 Ports

[Diagnostics > Ports]

The menu contains the following dialogs:

- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring

6.4.1 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 16.

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.

6.4.2 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 16.

Buttons

Reset

Opens the *Which statistic should be deleted?* window. The window displays the ports that you can enable again and reset the related counters to `0`. Click and select a table row to enable the corresponding port again.

This affects the counters in the following dialogs:

- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab
- *Diagnostics > Ports > Auto-Disable* dialog

Port

Displays the port number.

Link flap on

Activates/deactivates the monitoring of link flaps on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors link flaps on the port.
  - If the device detects too many link flaps, then the device executes the action specified in the *Action* column.
  - On the *Link flap* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

CRC/Fragments on

Activates/deactivates the monitoring of CRC/fragment errors detected on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors CRC/fragment errors detected on the port.
  - If the device detects too many CRC/fragment errors, then the device executes the action specified in the *Action* column.
  - On the *CRC/Fragments* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Duplex mismatch detection active

Activates/deactivates the monitoring of duplex mismatches on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors duplex mismatches on the port.
  - If the device detects a duplex mismatch, then the device executes the action specified in the *Action* column.
- `unmarked` (default setting)
  Monitoring is inactive.

Overload detection on

Activates/deactivates the overload detection on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors the data load on the port.
  - If the device detects a data overload on the port, then the device executes the action specified in the *Action* column.
  - On the *Overload detection* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Link speed/Duplex mode detection on

Activates/deactivates the monitoring of the link speed and duplex mode on the port.

Possible values:

- `marked`
  Monitoring is active.
  - The *Port Monitor* function monitors the link speed and duplex mode on the port.
  - If the device detects an unpermitted combination of link speed and duplex mode, then the device executes the action specified in the *Action* column.
  - On the *Link speed/Duplex mode detection* tab, specify the parameters to be monitored.
- `unmarked` (default setting)
  Monitoring is inactive.

Active condition

Displays the monitored parameter that led to the action on the port.

Possible values:

- `-`
  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 16.

Reason

Displays the parameters monitored by the *Port Monitor* function.

Mark the adjacent checkbox so that the *Port Monitor* function carries out the `auto-disable` action if it detects that the monitored parameters have been exceeded.

Auto-disable

Activates/deactivates the *Auto-Disable* function for the adjacent parameters.

Possible values:

- `marked`
  The *Auto-Disable* function for the adjacent parameters is active.
  If the adjacent parameters are exceeded and the value `auto-disable` is specified in the *Action* column, then the device carries out the *Auto-Disable* function.
- `unmarked` (default setting)
  The *Auto-Disable* function for the adjacent parameters is inactive.

[Link flap]

In this tab you specify individually for every port the following settings:
- The number of link changes.
- The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see how many link changes the *Port Monitor* function has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *Link flap on* column is marked on the *Global* tab.

Table

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

Port

Displays the port number.

Sampling interval [s]

Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

Possible values:

- `1..180` (default setting: `10`)

Link flaps

Specifies the number of link changes.

If the *Port Monitor* function detects this number of link changes in the monitored period, then the device performs the specified action.

Possible values:

- `1..100` (default setting: `5`)

Last sampling interval

Displays the number of errors that the device has detected during the period that has elapsed.

Total

Displays the total number of errors that the device has detected since the port was enabled.

[CRC/Fragments]

In this tab you specify individually for every port the following settings:

- The detected fragment error rate.
- The period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

You also see the fragment error rate that the device has detected up to now.

The *Port Monitor* function monitors those ports for which the checkbox in the *CRC/Fragments on* column is marked on the *Global* tab.

Table

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

Port

Displays the port number.

Sampling interval [s]

Specifies in seconds, the period during which the *Port Monitor* function monitors a parameter to detect discrepancies.

Possible values:

- `5..180` (default setting: `10`)

CRC/Fragments count [ppm]

Specifies the detected fragment error rate (in parts per million).

If the *Port Monitor* function detects this fragment error rate in the monitored period, then the device performs the specified action.

Possible values:

- `1..1000000 (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 16.

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 16.

Port

Displays the port number.

10M HDX

Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

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 HDX

Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- `marked`
  The port monitor takes into consideration the speed and duplex combination.
- `unmarked`
  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the *Global* tab.

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.

6.4.3 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 16.

Buttons

Reset

Opens the *Which statistic should be deleted?* window. The window displays the ports that you can enable again and reset the related counters to `0`. Click and select a table row to enable the corresponding port again.

This affects the counters in the following dialogs:
- *Diagnostics > Ports > Auto-Disable* dialog
- *Diagnostics > Ports > Port Monitor* dialog
  - *Link flap* tab
  - *CRC/Fragments* tab
  - *Overload detection* tab

Port

Displays the port number.

Reset timer [s]

Specifies the waiting period in seconds, after which the *Auto-Disable* function enables the port again.

Possible values:

- `0` (default setting)
  The timer is inactive. The port remains disabled.
- `30..4294967295 (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.
- `DOT1S`
  BPDU guard
  See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.

Reason

Displays the monitored parameter that led to the port being disabled.

Possible values:

- *none*
  No monitored parameter.
  The port is enabled.
- *Link flap*
  Too many link changes. See the *Diagnostics > Ports > Port Monitor* dialog, *Link flap* tab.
- *CRC error*
  Too many CRC/fragment errors are detected. See the *Diagnostics > Ports > Port Monitor* dialog, *CRC/Fragments* tab.
- *Duplex mismatch*
  Duplex mismatch detected. See the *Diagnostics > Ports > Port Monitor* dialog, *Global* tab.
- *BPDU rate*
  STP-BPDUs received. See the *Switching > L2-Redundancy > Spanning Tree > Global* dialog.
- *MAC-based port security*
  Too many data packets from undesired senders. See the *Network Security > Port Security* dialog.

- *Overload detection*
  Overload. See the *Diagnostics > Ports > Port Monitor* dialog, *Overload detection* tab.
- *Speed duplex*
  Impermissible combination of speed and duplex mode detected. See the *Diagnostics > Ports > Port Monitor* dialog, *Link speed/Duplex mode detection* tab.

Active

Displays if the port is currently disabled due to the parameters being exceeded.

Possible values:

- marked
  The port is currently disabled.
- unmarked
  The port is enabled.

[Status]

This tab displays the monitored parameters for which the *Auto-Disable* function is active.

Table

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

Reason

Displays the parameters that the device monitors.

Mark the adjacent checkbox so that the *Auto-Disable* function disables and, when applicable, enables the port again if the monitored parameters are exceeded.

Category

Displays which function the adjacent parameter belongs to.

Possible values:

- *port monitor*
  The parameter belongs to the functions in the *Diagnostics > Ports > Port Monitor* dialog.
- *network security*
  The parameter belongs to the functions in the *Network Security* dialog.
- *l2 redundancy*
  The parameter belongs to the functions in the *Switching > L2-Redundancy* 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.

6.4.4 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.

Allow management

Activates/deactivates the access to the device management using the destination port.

Possible values:

- `marked`
  The access to the device management using the destination port is active.
  The device lets users have access to the device management using the destination port without interrupting the active *Port Mirroring* session.
  - The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.
  - The VLAN settings on the destination port remain unchanged. The prerequisite for access to the device management using the destination port is that the destination port is not a member of the VLAN of the device management.
- `unmarked` (default setting)
  The access to the device management using the destination port is inactive.
  The device prohibits the access to the device management using the destination port.

Table

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

Source port

Displays the port number.

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.
  Verify that the *PTP* function is disabled on this port.
- *rx*
  Data packets that the source port receives.
  Verify that no *SFlow* sampler is active on this port.
- *txrx*
  Data packets that the source port sends.
  Verify that the *PTP* function is disabled on this port.

  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 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

6.5.1 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 16.

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.

6.5.2 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 16.

Port

Displays the port number.

Neighbor identifier

Displays the chassis ID of the neighboring device. This can be the basis MAC address of the neighboring device, for example.

FDB

Displays if the connected device has active LLDP support.

Possible values:

- `marked`
  The connected device does not have active LLDP support.
  The device uses information from its 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 16.

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.

6.6 Report

[Diagnostics > Report]

The menu contains the following dialogs:

- Report Global
- Persistent Logging
- System Log
- Audit Trail

6.6.1 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 372.

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 372.

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 372.

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 372.

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 372.

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

6.6.2 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:

- *usb*
  External USB memory (ACA22-USB-C (EEC))

Table

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

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.

6.6.3 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.

6.6.4 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
- Industrial Protocols
- 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 16.

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 16.

Buttons

 Add

Adds a table row.

 Remove

Removes the selected table row.

Index

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

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 16.

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 16.

Port

Displays the port number.

Active

Activates/deactivates the *DHCP L2 Relay* function on the port.

The prerequisite is that you enable the function globally.

Possible values:

- `marked`
  The *DHCP L2 Relay* function is active.
- `unmarked` (default setting)
  The *DHCP L2 Relay* function is inactive.

Trusted port

Activates/deactivates the secure *DHCP L2 Relay* mode for the corresponding port.

Possible values:

- `marked`
  The device accepts DHCPv4 packets with *Option 82* information.
  The device accepts DHCPv6 packets with *Option 18* information.
- `unmarked` (default setting)
  The device discards DHCPv4 packets received on non-secure ports that contain *Option 82* information.
  The device discards DHCPv6 packets received on ports that do not contain *Option 18* information.

[VLAN ID]

Table

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

VLAN ID

VLAN to which the table row relates.

Active

Activates/deactivates the *DHCP L2 Relay* function 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 16.

Buttons

Reset

Resets the counter for the statistics to `0`.

Port

Displays the port number.

Untrusted server messages with Option 82

Displays the number of DHCP server messages received with *Option 82* information on the untrusted interface.

Untrusted client messages with Option 82

Displays the number of DHCP client messages received with *Option 82* information on the untrusted interface.

Trusted server messages without Option 82

Displays the number of DHCP server messages received without *Option 82* information on the trusted interface.

Trusted client messages without Option 82

Displays the number of DHCP client messages received without *Option 82* information on the trusted interface.

7.3 Industrial Protocols

[Advanced > Industrial Protocols]

The menu contains the following dialogs:

- IEC 61850/MMS
- Modbus TCP
- EtherNet/IP
- PROFINET

7.3.1 IEC 61850/MMS

[Advanced > Industrial Protocols > IEC 61850/MMS]

IEC 61850/MMS is a standardized industrial communication protocol from the International Electrotechnical Commission (IEC). For example, automatic switching equipment uses this protocol when communicating with power station equipment.

The packet orientated protocol defines a uniform communication language based on the transport protocol, TCP/IP. The protocol uses a Manufacturing Message Specification (MMS) server for client server communications. The protocol includes functions for SCADA, Intelligent Electronic Device (IED) and the network control systems.

Note:
IEC 61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. As a result, incorrect device settings and potential network interruptions may occur.
Activate the write access only if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

This dialog lets you specify the following MMS server settings:
- Activates/deactivates the MMS server.
- Activates/deactivates the write access to the MMS server.
- The MMS server TCP Port.
- The maximum number of MMS server sessions.

Operation

Operation

Enables/disables the *IEC 61850/MMS* server.

Possible values:

- *On*
  The *IEC 61850/MMS* server is enabled.
- *Off* (default setting)
  The *IEC 61850/MMS* server is disabled.
  The IEC 61850 MIBs stay accessible.

Information

Status

Displays the current *IEC 61850/MMS* server status.

Possible values:

- *unavailable*
- *starting*
- *running*
- *stopping*

- *halted*
- *error*

Active sessions

Displays the number of active MMS server connections.

Configuration

Buttons

Download ICD file

Copies the ICD file to your PC.

Download CID file

Copies the CID file to your PC.

Write access

Activates/deactivates the write access to the MMS server.

Possible values:

- `marked`
  The write access to the MMS server is activated. This setting lets you change the device settings using the IEC 61850/MMS protocol.
- `unmarked` (default setting)
  The write access to the MMS server is deactivated. The MMS server is accessible as read-only.

IED name

Specifies the Intelligent Electronic Device (IED) name, also known as Technical Key.

The IED name is eligible independently of the system name.

Possible values:

- Alphanumeric ASCII character string with 0..32 characters
  The device accepts the following characters:
  - `_`
  - `0..9`
  - `a..z`
  - `A..Z` (default setting: `KEY`)

To get the MMS server to use the IED name, click the button and restart the MMS server. The connection to connected clients is then interrupted.

TCP port

Specifies TCP port for MMS server access.

Possible values:

- `1..65535 (2¹⁶-1)` (default setting: `102`)
  Exception: Port `2222` is reserved for internal functions.

Note:
The server restarts automatically after you change the port. In the process, the device terminates open connections to the server.

Sessions (max.)

Specifies the maximum number of MMS server connections.

Possible values:

- `1..15` (default setting: `5`)

7.3.2 Modbus TCP

[Advanced > Industrial Protocols > Modbus TCP]

Modbus TCP is a protocol used for Supervisory Control and Data Acquisition (SCADA) system integration. *Modbus TCP* is a vendor-neutral protocol used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLC), sensors and meters.

This dialog lets you specify the parameters of the protocol. To monitor and control the parameters of the device, you need an application with an Human-Machine Interface and the memory mapping table. Refer to the tables located in the “Configuration” user manual for the supported objects and memory mapping.

In the dialog, you can enable the function, activate the write access, and specify on which TCP port the Human-Machine Interface polls for data. You can also specify the number of sessions that can be open at the same time.

Note:
Activating the *Modbus TCP* write-access can cause a security risk, because the protocol does not authenticate user access.

To help minimize the security risks, specify the IP address range located in the *Device Security* > Management Access dialog. Enter only the IP addresses assigned to your devices before enabling the function. Furthermore, the default setting for monitoring function activation in the *Diagnostics* > Status Configuration > *Security Status* dialog, *Global* tab, is active.

Operation

Operation

Enables/disables the *Modbus TCP* server in the device.

Possible values:

- *On*
  The *Modbus TCP* server is enabled.
- *Off* (default setting)
  The *Modbus TCP* server is disabled.

Configuration

Write access

Activates/deactivates the write access to the *Modbus TCP* parameters.

Note:
Activating the *Modbus TCP* write-access can cause a security risk, because the protocol does not authenticate user access.

Possible values:

- `marked` (default setting)
  The *Modbus TCP* server read/write access is active. This lets you change the device settings using the *Modbus TCP* function.
- `unmarked`
  The *Modbus TCP* server read-only access is active.

TCP port

Specifies the TCP port number that the *Modbus TCP* server uses for communication.

Possible values:

- `<TCP Port number>` (default setting: `502`)
  Specifying `0` is not allowed.

Sessions (max.)

Specifies the maximum number of concurrent sessions that the *Modbus TCP* server maintains.

Possible values:

- `1..5` (default setting: `5`)

7.3.3 EtherNet/IP

[Advanced > Industrial Protocols > EtherNet/IP]

This dialog lets you specify the *EtherNet/IP* settings. You have the following options:
- Enable/disable the *EtherNet/IP* function in the device.
- Specify a VLAN which forwards the *EtherNet/IP* packets exclusively.
- Activate/deactivate the read/write capability of the *EtherNet/IP* function.
- Download the Electronic Data Sheet (EDS) file from the device.

Operation

Operation

Enables/disables the *EtherNet/IP* function in the device.

Possible values:

- *On*
  The *EtherNet/IP* function is enabled.
- *Off* (default setting)
  The *EtherNet/IP* function is disabled.

Configuration

Buttons

Download EDS file

Copies the following information in a zip file onto your PC:
- Electronic Data Sheet (EDS) with device related information
- Device icon

Write access

Activates/deactivates the read/write capability of the *EtherNet/IP* function.

Possible values:

- `marked`
  The *EtherNet/IP* function accepts set/get requests.
- `unmarked` (default setting)
  The *EtherNet/IP* function accepts only get requests.

VLAN Configuration

VLAN ID

Specifies the VLAN to be used for the *EtherNet/IP* function.

Possible values:

- `mgmt` (default setting)
  The *EtherNet/IP* function uses the VLAN, in which the device management is accessible through the network. You specify this VLAN in the *Basic Settings > Network > Global* dialog, *Management interface* frame, *VLAN ID* field.
- `1..4042`
  The *EtherNet/IP* function uses the selected VLAN.
  Prerequisites:
  - The VLAN is already set up in the device.
    See the *Switching > VLAN > Configuration* dialog.
  - The port over which the device forwards the *EtherNet/IP* packets is a member of the VLAN you assign and transmits the data packets with a VLAN tag.
    See the *Switching > VLAN > Configuration* dialog.
  - The *IP Access Restriction* function is enabled.
    See the *Device Security > Management Access > IP Access Restriction* dialog.

7.3.4 PROFINET

[Advanced > Industrial Protocols > PROFINET]

This dialog lets you set up the PROFINET protocol on this device used in conjunction with PROFINET Controllers and PROFINET devices. The device bases the *PROFINET* function on the Siemens V2.2 PROFINET stack for common Ethernet controllers. The PROFINET protocol implemented in the device conforms to Class B for real time responses according to IEC 61158.

Prerequisites for using the PROFINET function

Functions that directly affect the *PROFINET* function require the following default values to be changed. If you have obtained the device as a specially available *PROFINET* variant, then these values are already predefined:

PROFINET

Advanced > Industrial Protocols > PROFINET dialog

- *Operation* frame
  Operation = `On`
- *Configuration* frame
  Name of station field = `<empty>`

Network

Basic Settings > Network > IPv4 dialog

- *Management interface* frame
  IP address assignment radio button = `Local`
- *HiDiscovery protocol v1/v2* frame
  Access drop-down list = `readOnly`
- *IP parameter* frame
  IP address field = `0.0.0.0`
  Netmask field = `0.0.0.0`
  Gateway address field = `0.0.0.0`

LLDP

Diagnostics > LLDP > Configuration dialog

- *Configuration* frame
  Transmit interval [s] field = `5`
  Transmit delay [s] field = `1`

Operation

Operation

Enables/disables the *PROFINET* function in the device.

Possible values:

- *On*
  The *PROFINET* function is enabled.
- *Off* (default setting)
  The *PROFINET* function is disabled.

Configuration

Buttons

Download GSDML file

Copies the GSDML file onto your PC.

Preserve VLAN-0 tag

Activates/deactivates preserving the VLAN tag in forwarded data packets if the received data packet contains a VLAN ID of `0` (*priority tagged* packet).

The prerequisite is that the *PROFINET* function is enabled. When you disable the *PROFINET* function later, the device automatically deactivates preserving the VLAN tag.

Data packets with VLAN ID of `0`, which the device generates itself, are sent including the VLAN tag, regardless of whether this function is active or not.

Possible values:

- `marked`
  The device preserves the VLAN tag when forwarding data packets that contain a VLAN ID of `0`.
- `unmarked` (default setting)
  The device does not preserve the VLAN tag when forwarding data packets that contain a VLAN ID of `0`

Name of station

Specifies the name of the device.

Possible values:

- Alphanumeric ASCII character string with 0..240 characters
  The device prohibits you from using a digit as the first character.

Information

Active application relations

Displays how many application relations are active.

Table

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

Port

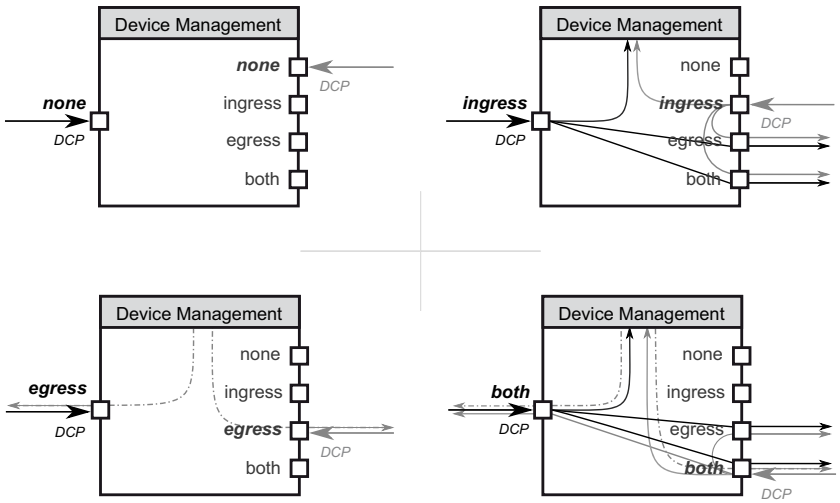
Displays the port number.

DCP mode

Specifies the data stream direction on the port to monitor for DCP packets.

The Programmable Logic Controllers (PLCs) detects PROFINET devices using the Discovery and Configuration Protocol (DCP).

The DCP identify request packets are multicast, the responses from the agents are unicast. Regardless of the settings, the device forwards the received DCP packets to other ports whose setting is either *egress* or *both*.



Possible values:

- *none*
  The agent does not respond to packets received on this port. The port does not forward packets received on other ports.
- *ingress*
  The agent responds to packets received on this port. The port does not forward packets received on other ports.

- *egress*
  The agent does not respond to packets received on this port. The port forwards packets received on other ports.
- *both* (default setting)
  The agent responds to packets received on this port. The port forwards packets received on other ports.

7.4 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 . . . 258
802.1X . . . 127, 163

A
Access control . . . 163
Access control lists . . . 197
Access restriction . . . 145
ACL . . . 197
Address conflict detection . . . 24, 329
Aging time . . . 209
Alarm . . . 317
ARP . . . 329
ARP table . . . 71, 333
Audit trail . . . 377
Authentication history . . . 176
Authentication list . . . 127
Auto disable . . . 159, 160, 282, 346, 347, 353

B
Boundary clock . . . 87
Bridge . . . 279

C
Cable diagnosis . . . 341
Certificate . . . 20, 44, 142, 143, 313
CLI . . . 150
Command line interface . . . 150
Community names . . . 152
Configuration check . . . 327
Configuration profile . . . 16, 40
Counter reset . . . 70

D
Daylight saving time . . . 74
Default gateway . . . 387
Device software . . . 36
Device software backup . . . 36
Device status . . . 19, 304
DHCP L2 Relay . . . 390
DHCP server . . . 379
DHCPv6 L2 Relay . . . 390
Digital certificate . . . 20, 44, 143, 313
DoS . . . 193
Download EDS for EtherNet/IP . . . 401
DSCP . . . 260
Duplicate Address Detection . . . 32

E
EAPOL 174
Egress rate limiter 211
Encryption 40
ENVM 39, 45, 47, 53, 374
EtherNet/IP 313, 401
EtherNet/IP, Download EDS 401
EtherNet/IP, Read/write capability 401
EtherNet/IP, VLAN 401
Event severity 372
External memory 22, 39, 45, 47, 53, 305, 306, 311, 374

F
Factory reset 44
FDB (MAC address table) 71, 214
Filter MAC addresses 214
Fingerprint 138, 142
Flash memory 39, 326
Flow control 209

G
GARP 250
GMRP 251
Guards 289
GVRP 253

H
Hardware clock 73
Hardware state 326
HiDiscovery 24, 312, 377
HIPER Ring 277
Host key 138
HTML 325, 376
HTTP 139
HTTP server 310
HTTPS 140

I
IAS 127, 178
IEC 61850/MMS 313, 396
IEEE 802.1X 127
IGMP snooping 71, 216
Industrial HiVision 9, 133
Ingress filtering 269
Ingress rate limiter 211
Integrated authentication server 127, 178
IP access restriction 145
IP address conflict detection 329
IP DSCP mapping 260
IPv4 rule 198

L
L2 Relay (DHCP) . . . 390
Link aggregation . . . 292
Link backup . . . 299
Link status . . . 305
LLDP . . . 359
Load/save . . . 40
Log file . . . 70, 71, 376
Login banner . . . 151, 153
Loops . . . 278

M
MAC Address Conflict Detection . . . 24
MAC flood . . . 158
MAC rule . . . 202
MAC spoof . . . 160
MAC address table (forwarding database) . . . 71, 214
Management access . . . 24, 30, 145
Management VLAN . . . 24
Manufacturing message specification . . . 396
Media redundancy protocol . . . 273
MMRP . . . 242
MMS . . . 396
Modbus TCP . . . 313, 399
MRP . . . 273
MRP-IEEE . . . 240
MRP-IEEE configuration . . . 241
MTU . . . 59
MVRP . . . 247

N
Network load . . . 61
NVM . . . 16, 39, 45

O
Out-of-band management port . . . 34

P
Password . . . 309
Password length . . . 118, 309
Password policy . . . 118
Persistent log file . . . 72
Persistent logging . . . 373
PoE . . . 62
Port clients . . . 172
Port configuration . . . 166, 256
Port mirroring . . . 357
Port monitor . . . 353
Port priority . . . 256
Port security . . . 158
Port statistics . . . 71, 174
Port VLAN . . . 268
Port-based access control . . . 163
Power over Ethernet . . . 62
Power supply . . . 21, 306
Pre-Login banner . . . 153
Priority queue . . . 255
PROFINET . . . 314, 403

Q

Queue management 262
Queues 255

R

RADIUS 127, 180
RAM 45
RAM self-test 335
Rate limiter 211
Read/write capability for EtherNet/IP 401
Reboot 70
Relay (DHCP) 390
Request interval 79
Reset the settings 44
Ring redundancy 306
Ring structure 273
Root bridge 279
RSTP 278, 279

S

Secure Boot 38, 314
Secure Shell (SSH) 135
Security status 20, 308
Self-test 335
Serial interface 311
Settings 40
Severity 372
SNMP server 133, 311
SNMP traps 59, 64, 66, 160, 279, 296, 304, 308, 317, 331, 346
SNMPv1/v2 152
SNTP 77
SNTP client 78
SNTP server 82
Software backup 36
Software update 36
Spanning tree protocol 278
SSH server 135
Support information 369
Support information (ZIP archive) 372
Syslog 337
System information 325
System log 376
System Monitor 1 335
System time 73

T
Technical Documents 415
Technical questions 415
Technical Support 415
Telnet server 134, 310
Temperature 21, 305
Threshold values network load 211
Time-Sensitive Networking 232
Topology discovery 364
Training courses 415
Transparent clock 96
Trap destination 322
Traps 59, 64, 66, 160, 279, 296, 304, 308, 317, 331, 346
Trust mode 256
TSN Configuration 232
TSN Gate Control List 236, 239
Twisted-pair 341

U
Unsigned device software (allow upload) 38
Uptime 21, 326
USB network interface 34
User administration 117
Utilization 61

V
Virtual local area network 263
VLAN 26, 31, 263
VLAN configuration 266
VLAN for EtherNet/IP 401
VLAN ports 268

W
Watchdog 40, 50
Web server 139, 140

Z
ZIP archive with support information 372

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
BOBCAT IP30/40 Extended Switch
HiOS-2S

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	42
1.5	Displaying a welcome message after user login	43
2	**Specifying the IP parameters**	45
2.1	IP parameter basics	45
2.1.1	IPv4	45
2.1.2	IPv6	49
2.2	Specifying the IP parameters using the Command Line Interface	54
2.2.1	IPv4	54
2.2.2	IPv6	55
2.3	Specifying the IP parameters using HiDiscovery	57
2.4	Specifying the IP parameters using the Graphical User Interface	59
2.4.1	IPv4	59
2.4.2	IPv6	60
2.5	Specifying the IP parameters using BOOTP	61
2.6	Specifying the IP parameters using DHCP	62
2.6.1	IPv4	62
2.6.2	IPv6	63
2.7	Management address conflict detection	65
2.7.1	Active and passive detection	65
2.8	Duplicate Address Detection function	66

3	**Access to the device**	67
3.1	First login (Password change)	67
3.2	Authentication lists	68
3.2.1	Applications	68
3.2.2	Policies	68
3.2.3	Managing authentication lists	68
3.2.4	Adjusting the settings	69
3.3	User management	71
3.3.1	Access roles	71
3.3.2	Managing user accounts	73
3.3.3	Default user accounts	73
3.3.4	Changing default passwords	73
3.3.5	Setting up a new user account	74
3.3.6	Automatic unlocking of user accounts	75
3.3.7	Deactivating the user account	77
3.3.8	Adjusting policies for passwords	77
3.4	SNMP access	79
3.4.1	SNMPv1/v2 access	79
3.4.2	SNMPv3 access	79
3.4.3	SNMPv3 traps	80
3.5	Out-of-Band access	83
3.5.1	Specifying the IP parameters	83
3.5.2	Disabling the USB network interface	84
4	**Synchronizing the system time in the network**	85
4.1	Setting the time	85
4.2	Automatic daylight saving time changeover	87
4.2.1	Setting daylight saving time using pre-defined profiles	87
4.2.2	Setting daylight saving time manually	87
4.3	Synchronizing time in the network with SNTP	89
4.3.1	Preparation	90
4.3.2	Defining settings of the SNTP client	90
4.3.3	Specifying SNTP server settings	92
4.4	Synchronizing time in the network with PTP	93
4.4.1	Types of clocks	93
4.4.2	Best Master Clock algorithm	94
4.4.3	Delay measurement	94
4.4.4	PTP domains	95
4.4.5	Using PTP	95
4.5	Synchronizing time in the network with 802.1AS	96
4.5.1	Instances and domains	96
4.5.2	Best Master Clock algorithm	96
4.5.3	Enabling the 802.1AS function	97
4.5.4	Disabling the 802.1AS function globally	98
4.5.5	Disabling the 802.1AS function for an instance	98
4.5.6	Disabling the 802.1AS function on a port	99
5	**Managing configuration profiles**	101
5.1	Detecting changed settings	101
5.1.1	Volatile memory (RAM) and non-volatile memory (NVM)	101
5.1.2	external memory (ENVM) and non-volatile memory (NVM)	102

5.2 Saving the settings . . . 103
5.2.1 Saving the configuration profile in the device . . . 103
5.2.2 Saving the configuration profile in the external memory (ENVM) . . . 105
5.2.3 Backing up the configuration profile on a remote server . . . 105
5.2.4 Exporting a configuration profile . . . 106
5.3 Loading settings . . . 108
5.3.1 Activating a configuration profile . . . 108
5.3.2 Loading the configuration profile from the external memory (ENVM) . . . 108
5.3.3 Importing a configuration profile . . . 110
5.4 Resetting the device to the default setting . . . 113
5.4.1 Using the Graphical User Interface or Command Line Interface . . . 113
5.4.2 Using System Monitor 1 . . . 113

6 Updating the device software . . . 115
6.1 Loading a previous device software version . . . 115
6.2 Software update from the PC . . . 116
6.3 Software update from a server . . . 117
6.3.1 Software update through FTP . . . 117
6.3.2 Software update through TFTP . . . 118
6.3.3 Software update through SFTP . . . 119
6.3.4 Software update through SCP . . . 121
6.4 Software update from the external memory (ENVM) . . . 123
6.4.1 Manually—initiated by the administrator . . . 123
6.4.2 Automatically—initiated by the device . . . 123

7 Configuring the ports . . . 125
7.1 Enabling/Disabling the port . . . 125
7.2 Selecting the operating mode . . . 126

8 Assistance in the protection from unauthorized access . . . 127
8.1 Changing the SNMPv1/v2 community . . . 127
8.2 Disabling SNMPv1/v2 . . . 128
8.3 Disabling HTTP . . . 129
8.4 Disabling Telnet . . . 130
8.5 Disabling the HiDiscovery access . . . 131
8.6 Restricting access to device management . . . 132
8.6.1 Restricting access from a specific IP address range . . . 132
8.7 Adjusting the session timeouts . . . 134
8.8 Customizing the SSH settings . . . 136
8.8.1 Generating the RSA host key in the device . . . 136
8.8.2 Transferring an externally generated private RSA key to the device . . . 137
8.9 Making SSH hosts known to the device . . . 140

9 Controlling the data traffic . . . 143
9.1 Helping protect against DoS attacks . . . 143
9.1.1 Filters for TCP and UDP packets . . . 144
9.1.2 Filters for IP packets . . . 147
9.1.3 Filters for ICMP packets . . . 147

9.2 ACL . . . 150
9.2.1 Creating and editing IPv4 rules . . . 151
9.2.2 Creating and configuring an IP ACL using the Command Line Interface . . . 152
9.2.3 Creating and editing MAC rules . . . 152
9.2.4 Creating and configuring a MAC ACL using the Command Line Interface . . . 153
9.2.5 Assigning ACLs to a port or VLAN . . . 154
9.2.6 Maximum number of rules that can be assigned . . . 154

10 Network load control . . . 157
10.1 Direct packet distribution . . . 157
10.1.1 Learning MAC addresses . . . 157
10.1.2 Aging of learned MAC addresses . . . 157
10.1.3 Static address entries . . . 158
10.2 Multicasts . . . 161
10.2.1 Example of a Multicast application . . . 161
10.2.2 IGMP snooping . . . 161
10.3 Rate limiter . . . 166
10.4 QoS/Priority . . . 167
10.4.1 Description of prioritization . . . 167
10.4.2 Handling of received priority information . . . 168
10.4.3 VLAN tagging . . . 168
10.4.4 IP ToS (Type of Service) . . . 169
10.4.5 Handling of traffic classes . . . 170
10.4.6 Queue management . . . 171
10.4.7 Management prioritization . . . 173
10.4.8 Setting prioritization . . . 174
10.5 Flow control . . . 178
10.5.1 Flow Control with a half-duplex link . . . 178
10.5.2 Flow Control with a full-duplex link . . . 179
10.5.3 Setting up the Flow Control . . . 179

11 Configuring template-based TSN . . . 181
11.1 Underlying facts . . . 181
11.2 Application example for template-based TSN . . . 182
11.2.1 Time calculation . . . 182
11.2.2 Setting up the devices . . . 182

12 VLANs . . . 185
12.1 Examples of VLANs . . . 185
12.1.1 Application example of a simple port-based VLAN . . . 186
12.1.2 Application example of a complex VLAN setup . . . 190
12.2 Guest VLAN / Unauthenticated VLAN . . . 195
12.3 RADIUS VLAN assignment . . . 197
12.4 Creating a Voice VLAN . . . 198

13 Redundancy . . . 199
13.1 Network Topology vs. Redundancy Protocols . . . 199
13.1.1 Network topologies . . . 199
13.1.2 Redundancy Protocols . . . 200
13.1.3 Combinations of redundancy protocols . . . 201

13.2 Media Redundancy Protocol (MRP) . . . 202
13.2.1 Network structure . . . 202
13.2.2 Reconfiguration time . . . 203
13.2.3 Advanced mode . . . 203
13.2.4 Prerequisites for MRP . . . 203
13.2.5 Advanced Information . . . 204
13.2.6 Application example of an MRP Ring . . . 205
13.3 HIPER Ring Client . . . 209
13.3.1 VLANS on the HIPER Ring . . . 209
13.3.2 Advanced Information . . . 210
13.4 Spanning Tree . . . 212
13.4.1 Basics . . . 212
13.4.2 Rules for Creating the Tree Structure . . . 216
13.4.3 Examples . . . 218
13.5 Rapid Spanning Tree Protocol . . . 221
13.5.1 Port roles . . . 221
13.5.2 Port states . . . 222
13.5.3 Spanning Tree Priority Vector . . . 223
13.5.4 Fast reconfiguration . . . 223
13.5.5 Configuring the device . . . 224
13.5.6 Guards . . . 226
13.6 Link Aggregation . . . 230
13.6.1 Methods of Operation . . . 230
13.6.2 Link Aggregation Example . . . 231
13.7 Link Backup . . . 232
13.7.1 Fail Back Description . . . 232
13.7.2 Application example for the Link Backup function . . . 232

14 Operation diagnosis . . . 235
14.1 Sending SNMP traps . . . 235
14.1.1 SNMP traps for configuration activity . . . 235
14.1.2 SNMP trap setting . . . 236
14.1.3 ICMP messaging . . . 236
14.2 Monitoring the Device Status . . . 237
14.2.1 Events which can be monitored . . . 237
14.2.2 Configuring the Device Status . . . 238
14.2.3 Displaying the Device Status . . . 239
14.3 Security Status . . . 240
14.3.1 Events which can be monitored . . . 240
14.3.2 Configuring the Security Status . . . 241
14.3.3 Displaying the Security Status . . . 243
14.4 Port event counter . . . 244
14.4.1 Detecting non-matching duplex modes . . . 244
14.5 Auto-Disable . . . 246
14.6 Topology discovery . . . 248
14.6.1 Displaying the Topology discovery results . . . 248
14.6.2 LLDP-Med . . . 249
14.7 Detecting loops . . . 250

14.8 Reports . . . 251
14.8.1 Global settings . . . 251
14.8.2 Syslog . . . 253
14.8.3 System Log . . . 254
14.8.4 Audit Trail . . . 256
14.9 Network analysis with TCPdump . . . 257
14.10 Monitoring the data stream with Port Mirroring . . . 258
14.10.1 Enabling the Port Mirroring function . . . 259
14.11 Self-test . . . 260
14.12 Copper cable test . . . 262

15 Advanced functions of the device . . . 263
15.1 DHCP server . . . 263
15.1.1 Settings that the server assigns to the clients . . . 263
15.1.2 Pools . . . 263
15.1.3 Setting up a Preboot eXecution Environment (PXE) . . . 266
15.2 DHCP L2 Relay . . . 268
15.2.1 Circuit and Remote IDs . . . 268
15.2.2 DHCP L2 Relay configuration . . . 269
15.3 GARP function . . . 272
15.3.1 Configuring GMRP . . . 272
15.3.2 Configuring GVRP . . . 273
15.4 MRP-IEEE . . . 274
15.4.1 MRP-IEEE operation . . . 274
15.4.2 MRP-IEEE timers . . . 274
15.4.3 MMRP . . . 275
15.4.4 MVRP . . . 277

16 Industry Protocols . . . 279
16.1 IEC 61850/MMS . . . 280
16.1.1 Switch model for IEC 61850 . . . 280
16.1.2 Integration into a Control System . . . 281
16.2 Modbus TCP function . . . 284
16.2.1 Client/Server Modbus TCP/IP Mode . . . 284
16.2.2 Supported Functions and Memory Mapping . . . 284
16.2.3 Application example for the Modbus TCP function . . . 289
16.3 EtherNet/IP function . . . 292
16.3.1 Integration into a Control System . . . 292
16.3.2 EtherNet/IP Entity Parameters . . . 293
16.4 PROFINET function . . . 310
16.4.1 Device Models for PROFINET GSDML Version 2.41 . . . 310
16.4.2 Graphical User Interface and Command Line Interface . . . 311
16.4.3 Integrating the device into a Control System . . . 311
16.4.4 Incorporating the device in the configuration . . . 313
16.4.5 Activating the Preserve VLAN-0 tag function . . . 367
16.4.6 PROFINET parameters . . . 367

A Setting up the configuration environment . . . 373
A.1 Setting up a DHCP/BOOTP server . . . 373
A.2 Setting up a DHCP server with Option 82 . . . 376

A.3 HTTPS certificate . . . 379
A.3.1 Conflicts in certificate validation . . . 379
A.3.2 HTTPS certificate management . . . 379
A.3.3 Access through HTTPS . . . 380

B Appendix . . . 383
B.1 Literature references . . . 383
B.2 Management Information Base (MIB) . . . 384
B.3 List of RFCs . . . 386
B.4 Underlying IEEE Standards . . . 389
B.5 Underlying IEC Norms . . . 390
B.6 Underlying ANSI Norms . . . 391
B.7 Technical Data . . . 392
B.7.1 Switching . . . 392
B.7.2 VLAN . . . 392
B.7.3 Access Control Lists (ACL) . . . 392
B.8 Copyright of integrated Software . . . 393
B.9 Abbreviations used . . . 394

C Index . . . 397

D Technical support . . . 403

E Readers' Comments . . . 404

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 108.
- The new device gets its IP address using DHCP *Option 82*.
  See “DHCP L2 Relay” on page 268.
  See “Setting up a DHCP server with Option 82” on page 376.

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 379.
- 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 137.

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 71.
- A remote server grants authorization
  – RADIUS

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 45.

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 67.
- ☐ 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

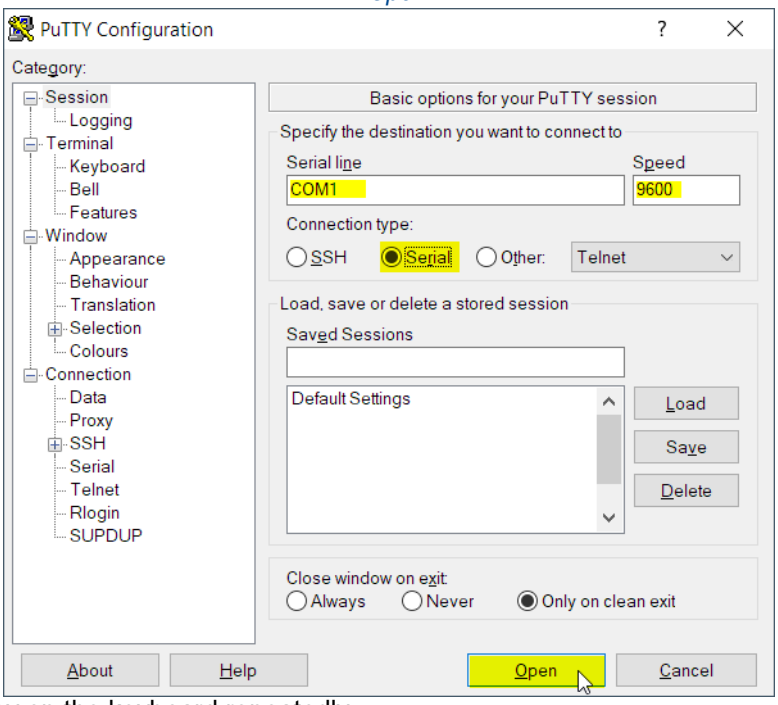
To access the device management, connect a management station with VT100 terminal emulation to the serial interface of the device.

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 67.

You are logged in to the device management.

```
                    Copyright (c) 2011-2026 Hirschmann Automation and Control GmbH

                                  All rights reserved

                              BXS40-1200 Release HiOS-2S-10.6.00

                                 (Build date 2026-10-03 09:34)


                    System Name   :  BXS40-ECE555d6e786
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    USB IP        :  192.168.248.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:45:50


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.

BXS>
```

Figure 1: Start screen of the Command Line Interface

1.2.2 Access to the device management using SSH

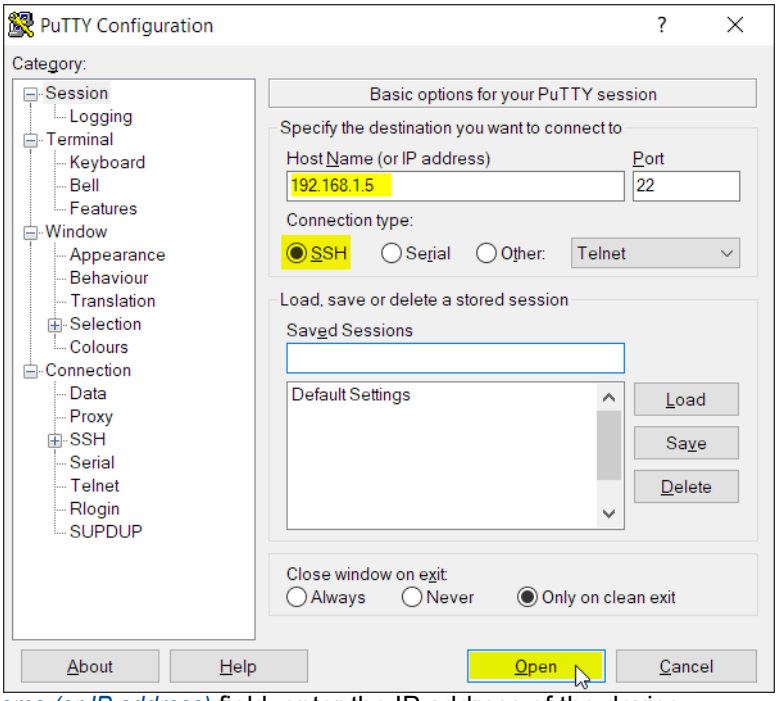
The prerequisite for accessing the device management is that the IP parameters are set up in the device. See “Specifying the IP parameters” on page 45.

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.

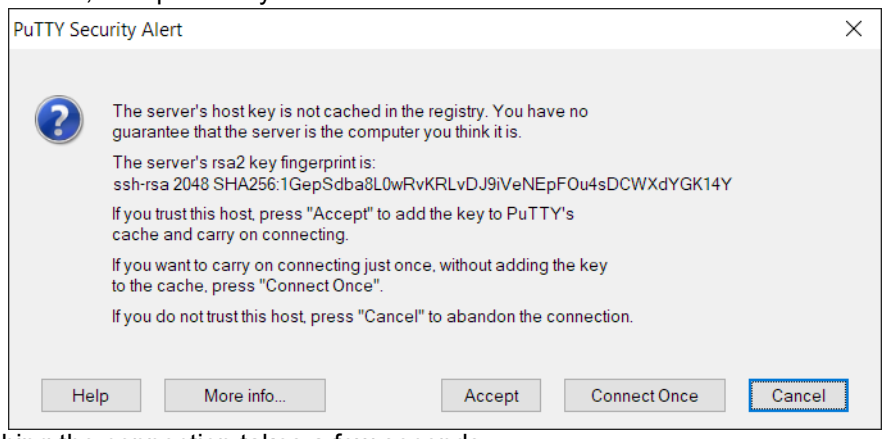


☐ In the *Host Name (or IP address)* field, enter the IP address of the device.
☐ In the *Connection type* option list, select the *SSH* radio button.
☐ Click the *Open* button.
When you connect the management station to the device for the first time, the SSH client application displays a *host key* 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 67.

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

                               BXS40-1200 Release HiOS-2S-10.6.00

                                  (Build date 2026-10-03 09:34)


                    System Name   :  BXS40-ECE555d6e786
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    USB IP        :  192.168.248.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:45:50


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.

BXS>
```

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.

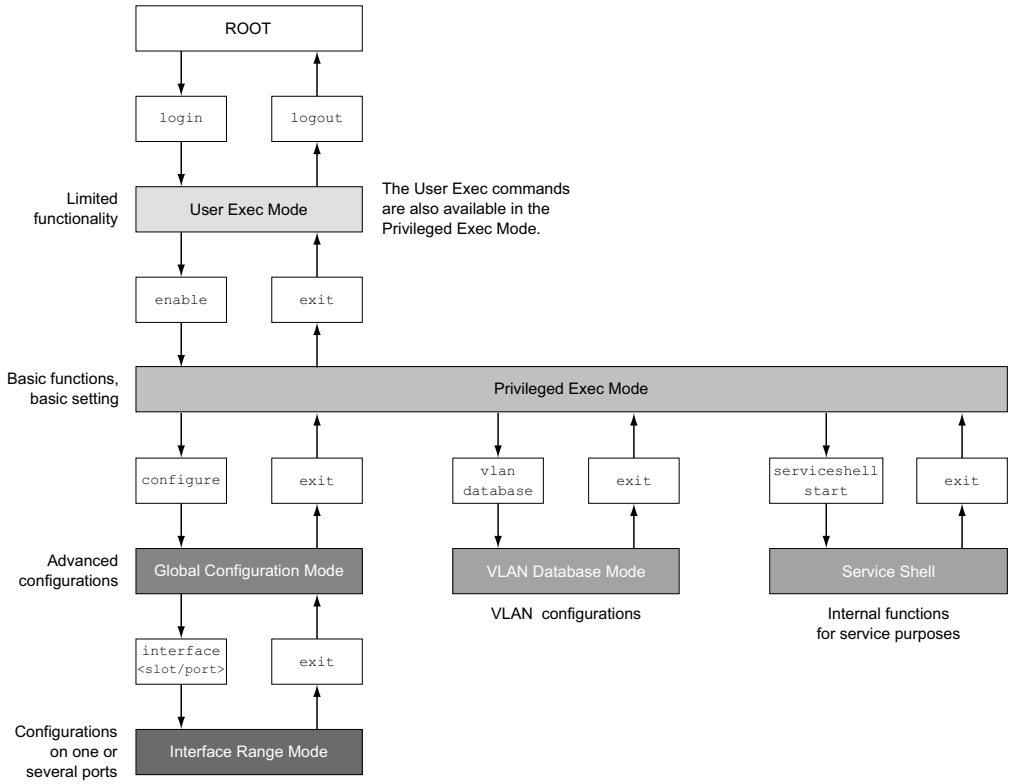


Figure 3: Structure of the Command Line Interface

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: `(BXS) >`
- *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:`(BXS) #`
- VLAN mode
  The VLAN mode contains VLAN-related commands.
  Command prompt: `(BXS) (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: `(BXS) (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: `(BXS) ((interface) all)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (BXS) (config)#interface all
    (BXS) ((Interface)all)#
    ```
  - A single port on one interface
    Command prompt: `(BXS) (interface <slot/port>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (BXS) (config)#interface 2/1
    (BXS) (interface 2/1)#
    ```
  - A range of ports on one interface
    Command prompt: `(BXS) (interface <interface range> )#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (BXS) (config)#interface 1/2-1/4
    (BXS) ((Interface)1/2-1/4)#
    ```
  - A list of single ports
    Command prompt: `(BXS) (interface <interface list>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (BXS) (config)#interface 1/2,1/4,1/5
    (BXS) ((Interface)1/2,1/4,1/5)#
    ```
  - A list of port ranges and single ports
    Command prompt: `(BXS) (interface <complex range>)#`
    Example: When you switch from the *Global Config* mode to the *Interface Range* mode, the command prompt changes as follows:
    ```
    (BXS) (config)#interface 1/2-1/4,1/6-1/9
    (BXS) ((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`:
		`(BXS) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec mode	From the *User Exec* mode, you enter the command `enable`:
	`(BXS) >enable`
	`(BXS) #`
		To quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit`:
		`(BXS) #exit`
		`(BXS) >`

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`:
	`(BXS) #vlan database`
	`(BXS) (Vlan)#`
		To end the VLAN mode and return to the *Privileged Exec* mode, you enter `exit` or press <CTRL>+<Z>.
		`(BXS) (Vlan)#exit`
		`(BXS) #`

Global Config mode	From the *Privileged Exec* mode, you enter the command `configure`:
	`(BXS) #configure`
	`(BXS) (config)#`
	From the *User Exec* mode, you enter the command `enable`, and then in *Privileged Exec* mode, enter the command `Configure`:
	`(BXS) >enable`
	`(BXS) #configure`
	`(BXS) (config)#`
		To quit the *Global Config* mode and return to the *Privileged Exec* mode, you enter `exit`:
		`(BXS) (config)#exit`
		`(BXS) #`
		To then quit the *Privileged Exec* mode and return to the *User Exec* mode, you enter `exit` again:
		`(BXS) #exit`
		`(BXS) >`

Interface Range mode	From the *Global Config* mode you enter the command `interface {all|<slot/port>|<interface range>|<interface list>|<complex range>}`.
	`(BXS) (config)#interface <slot/port>`
	`(BXS) (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>.
		`(BXS) (interface slot/port)#exit`
		`(BXS) #`

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.

```
(BXS)>
  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.

(BXS)>
```

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 `(BXS)>` 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:

```
(BXS)>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:

```
*(BXS)#cli prompt Device name
Error: Invalid command 'name'

*(BXS)#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.

```
(BXS) (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.

```
(BXS) (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:

- `(BXS) >`
  User Exec mode
- `(BXS) #`
  Privileged Exec mode
- `(BXS) (config)#`
  Global Config mode
- `(BXS) (Vlan)#`
  VLAN Database mode
- `(BXS) ((Interface)all)#`
  Interface Range mode / All ports of the device
- `(BXS) ((Interface)2/1)#`
  Interface Range mode / A single port on one interface
- `(BXS) ((Interface)1/2-1/4)#`
  Interface Range mode / A range of ports on one interface
- `(BXS) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / A list of single ports
- `(BXS) ((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.
  `*(BXS)>`
- 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.
  *#`(BXS)>`
- 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.
  `!(BXS)>`

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

```
!(BXS)>enable

!(BXS)#cli prompt %i

!192.168.1.5#cli prompt (BXS)%d

!*(BXS)2026-10-05#cli prompt (BXS)%d%t

!*(BXS)2026-10-05 12:45:50#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:

```
(BXS) #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

(BXS) #
```

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:
  ```
  (BXS) (Config)#lo
  (BXS) (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 `(BXS) >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:

```
!*#(BXS)(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: `(BXS) >`

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.

```
!BXS >enable

!*BXS #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 12:45:50 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: `(BXS) >`

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.

```
!BXS >enable

!*BXS #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 USB-C 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

During system startup, the serial connection to the device is unavailable through the USB-C interface. For this reason, accessing System Monitor 1 works differently from other Hirschmann devices.

To change to System Monitor 1, perform the following steps:
- ☐ “Putting the device into Recovery Mode” on page 39
- ☐ “Changing to System Monitor 1” on page 40

Putting the device into Recovery Mode

Required accessories:
- External memory (recommended: ACA22-USB-C (EEC))
- USB-C to USB-A adapter (only when you use an external memory device (*ENVM*) other than the recommended one)

Perform the following steps:
- ☐ Plug the external memory (*ENVM*) into the management station.
- ☐ Create an empty file `recovery.txt` in the root directory of the external memory (*ENVM*).
- ☐ Plug the external memory (*ENVM*) into the device.
- ☐ Restart the device.

☐ Observe the LEDs while the device boots. When the *Status* LED flashes alternately red and green, the device has successfully booted into the Recovery Mode.

Note:
You find the description of the display elements in the “Installation” user manual.

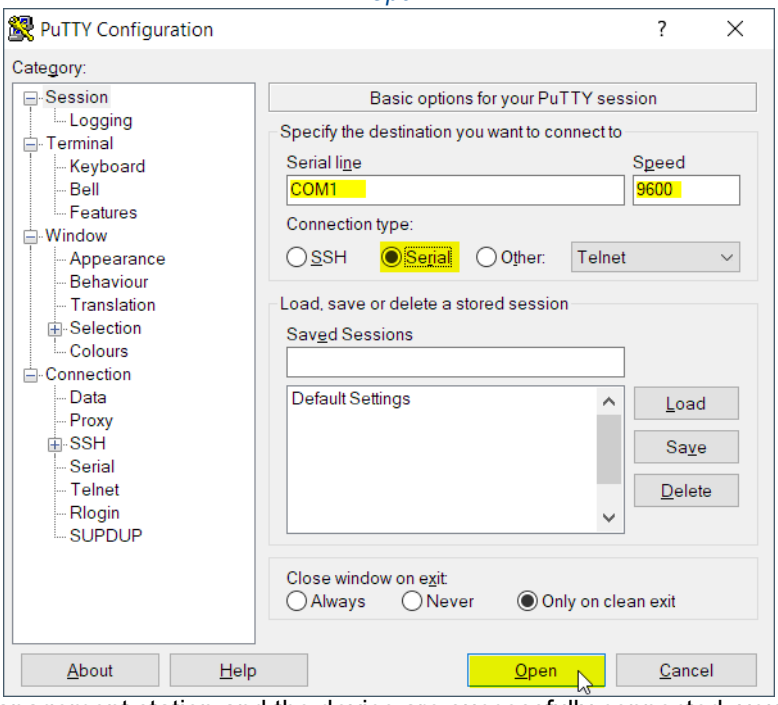
☐ Remove the external memory from the device.

Changing to System Monitor 1

Required accessories:
- USB cable to connect the management station to the USB-C interface of the device
- Management station with VT100 terminal emulation

Perform the following steps:
☐ Connect the management station to the device over the USB cable.
☐ On the management station, start the VT100 terminal emulation.

☐ Set up the serial connection. Then click the *Open* button.



When the management station and the device are successfully connected, you see a blank screen.

☐ Press the <Enter> key.
After a few seconds, the VT100 terminal emulation displays the System Monitor 1 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.

Note:
If you intend to leave the external memory (*ENVM*) permanently plugged in to the device, first delete the file `recovery.txt` from the root directory of the external memory (*ENVM*).

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 43.

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 42.

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

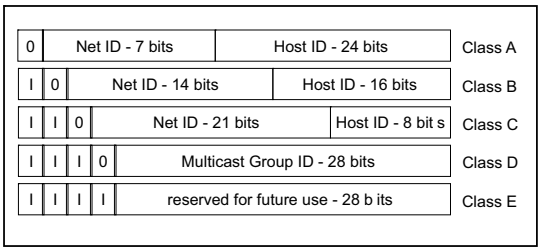


Figure 6: Bit representation of the IP address

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?

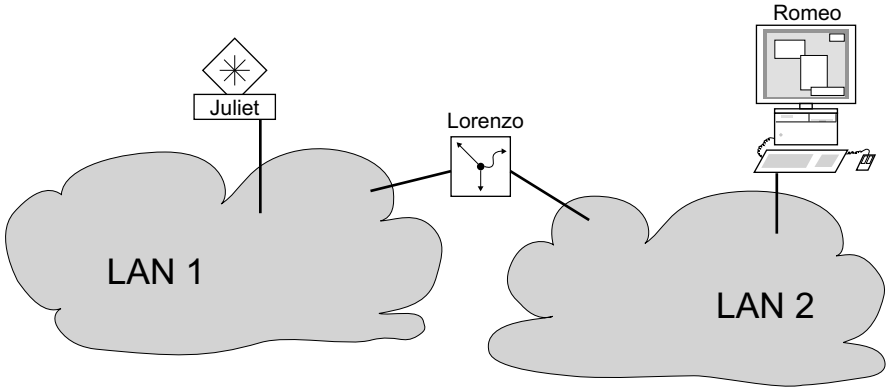


Figure 7: The management agent is separated from its network management station by a router

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.

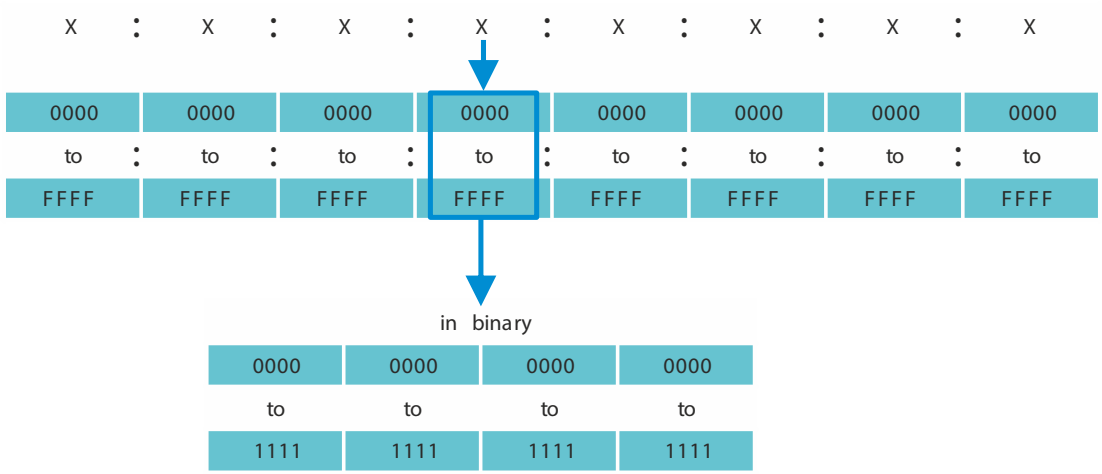


Figure 8: IPv6 address representation

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

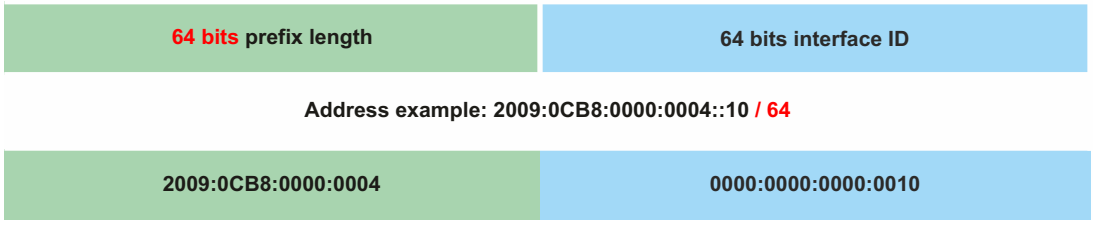
Unlike an IPv4 address, an IPv6 address does not use a subnet mask to identify the subnet part of the address. Instead, the IPv6 protocol uses the prefix length.

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.

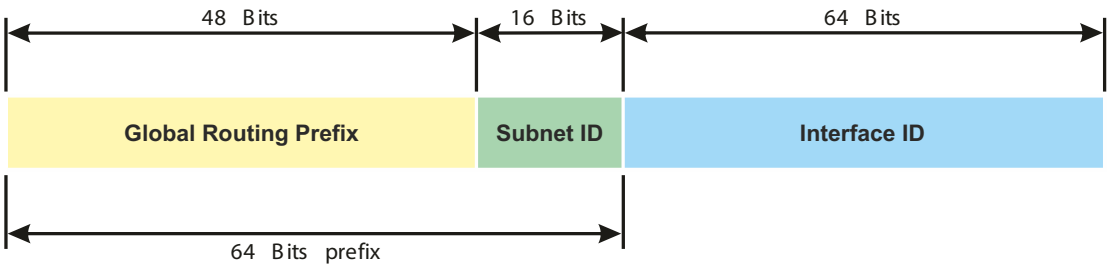


Figure 9: IPv6 Global Unicast address general format

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

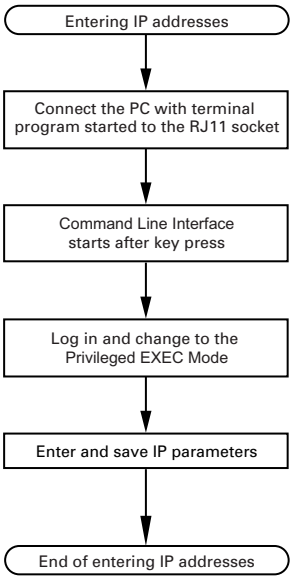
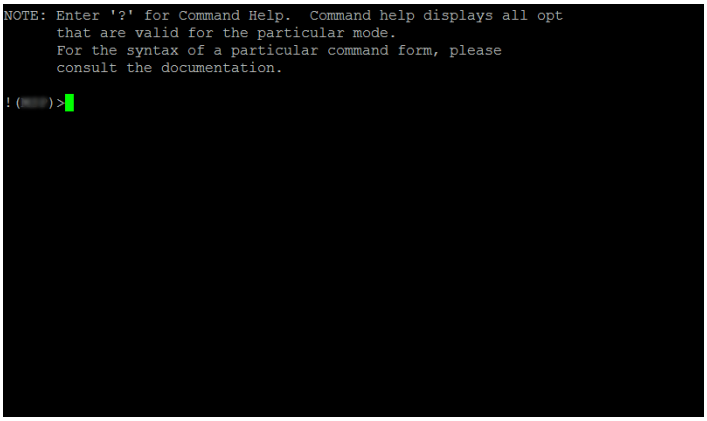


Figure 10: Flow chart for entering IP addresses

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 47 “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.

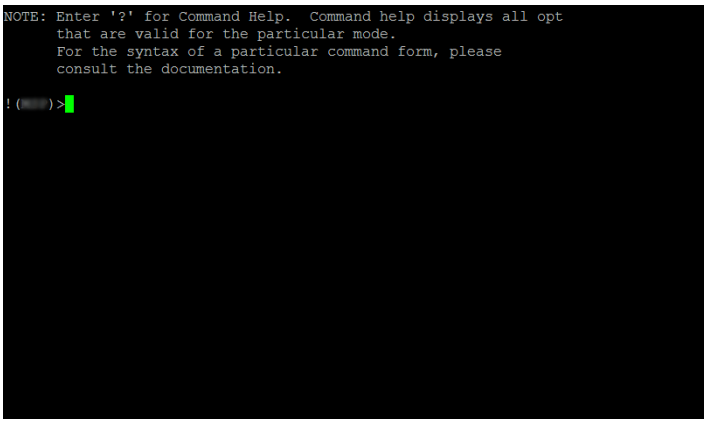
After entering the IP parameters, you easily set up the device using the Graphical User Interface.

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 51 “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.

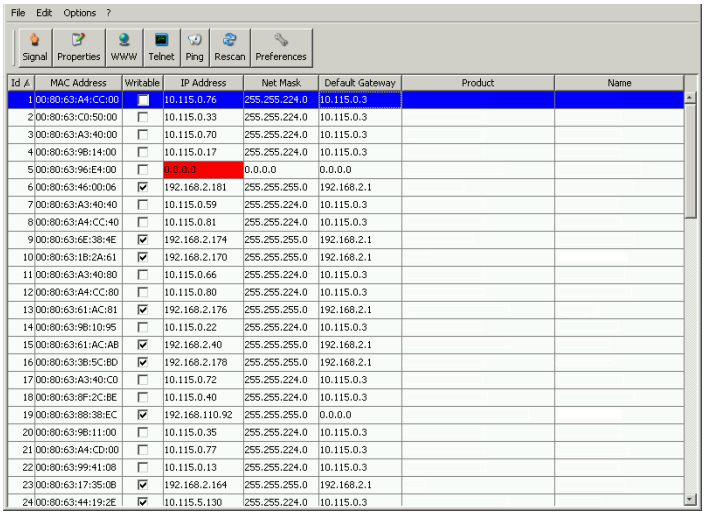


Figure 11: HiDiscovery

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.

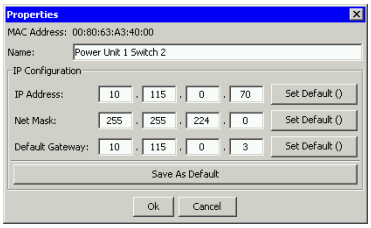


Figure 12: HiDiscovery – assigning IP parameters

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 66 “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
- RADIUS

When the end device logs in with valid login data, the device lets the connected end devices have access to the network with the port-based access control according to IEEE 802.1X. The device authenticates the end devices using the following policies:
- RADIUS
- IAS (Integrated Authentication Server)

The device gives you the option of a fall-back solution. For this, you specify more than one policy in the authentication list. When authentication is unsuccessful using the current policy, the device applies the next specified policy.

3.2.3 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.

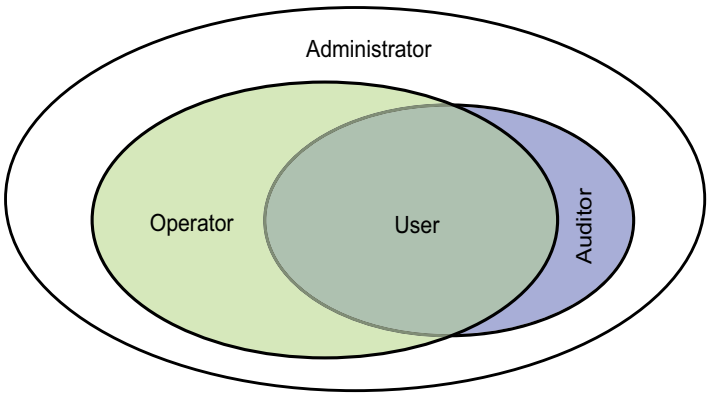


Figure 13: Access roles for user accounts

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 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.

3.4.1 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.
- ☐ We recommend using SNMPv3 and disabling the access using SNMPv1 and SNMPv2 in the device.

3.4.2 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.

3.4.3 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 73.

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.

3.5 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.

The prerequisite is that you connect the management station directly to the USB port. When you use Microsoft Windows, install the RNDIS driver, where necessary. As soon as you connect the management station, it can communicate with the device management over a virtual network connection.

In the default setting, you can access the device management through this port using the following IP parameters:
- *IP address* `192.168.248.100`
- *Netmask* `255.255.255.0`

The device lets you access the device management using the following protocols:
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP
- Industry protocols
  - *IEC 61850/MMS*
  - *Modbus TCP*
  - *EtherNet/IP*

3.5.1 Specifying the IP parameters

When you connect the management station through the USB port, the device assigns the IP address of the USB network interface, increased by 1, to the management station (`192.168.248.101` in the default setting). The device lets you change the IP parameters to adapt the device to the requirements of your environment.

Verify that the IP subnet of this network interface 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 USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out-of-Band over USB* dialog.
- ☐ Overwrite the IP address in the *IP parameter* frame, *IP address* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

```
enable
```
To change to the Privileged EXEC mode.

```
network usb parms 192.168.1.1 255.255.255.0
```
To specify the IP address `192.168.1.1` and the netmask `255.255.255.0` for the USB network interface.

```
show network usb
```
To display the USB network interface settings.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86
```

```
save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

3.5.2 Disabling the USB network interface

In the default setting, the USB network interface is enabled. If you do not want someone to access device management through the USB port, then the device lets you disable the USB network interface.

If the management station accesses the device management through the USB port, then the device disconnects the Graphical User Interface and Command Line Interface immediately after you have performed the changes.

Perform the following steps:

- ☐ Open the *Basic Settings > Out-of-Band over USB* dialog.
- ☐ Disable the USB 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 usb operation
```
To disable the USB network interface.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86
```

```
save
```
To save the settings in the non-volatile memory (`nvm`) in the “Selected” configuration profile.

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
- 802.1AS 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.

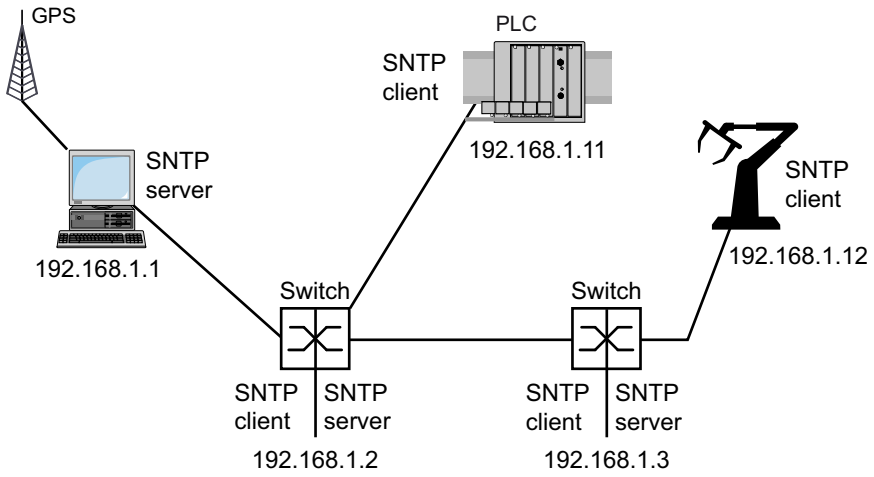


Figure 14: Example of SNTP cascade

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).

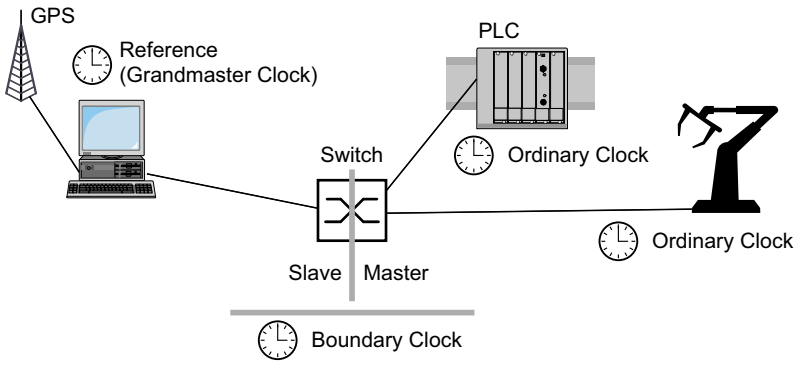


Figure 15: Position of the boundary clock in a network

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.

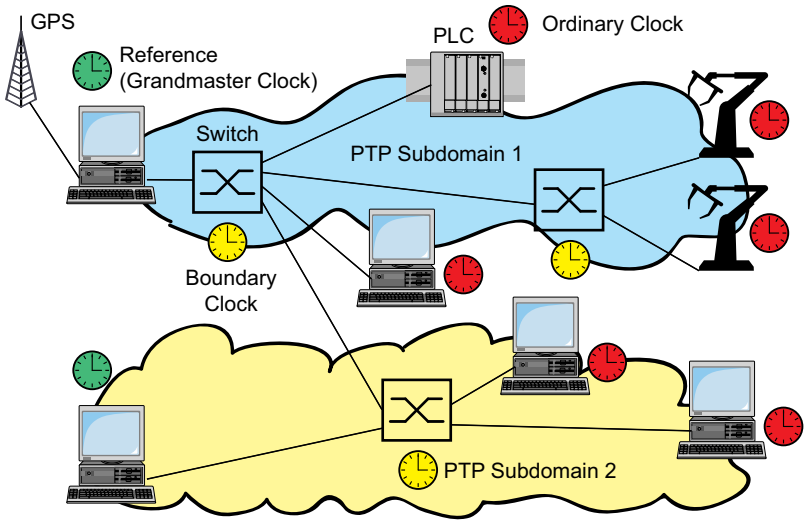


Figure 16: Example of PTP domains

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*.

4.5 Synchronizing time in the network with 802.1AS

Some LAN-based applications require the internal clocks of the participating devices to be precisely synchronized. The IEEE 802.1AS-2020 protocol describes a method that enables precise synchronization of the clocks of time-aware devices in the network.

The IEEE 802.1AS-2020 protocol is based on Precision Time Protocol (PTP) and is tailored for Ethernet-based Time-Sensitive Networking (TSN) environments.

The *802.1AS* function in the device permits time synchronization with an accuracy of a few 100 ns. The *802.1AS* function uses Multicasts for the synchronization messages, therefore keeping the network load low.

4.5.1 Instances and domains

Each *PTP domain* operates independently and helps ensure that the clocks of the time-aware devices within the *PTP domain* are synchronized. The devices are synchronized to the reference time source (*Grandmaster*) of the respective domain. You can use different domains to synchronize the time for different groups of devices within a network.

The device can be part of multiple *PTP domains*. In the device, the *802.1AS* function supports 2 instances: *Instance 0* and *Instance 1*, each operating within separate *PTP domains*.

You set up each instance separately:
- *Instance 0*
  for synchronizing device clocks and transmitting time synchronization messages
- *Instance 1*
  only for transmitting time synchronization messages

4.5.2 Best Master Clock algorithm

The devices participating in PTP designate a device in the *PTP domain* as a reference time source (*Grandmaster*). The *Best Master Clock* algorithm is used to determine the accuracy of the clocks available in the *PTP domain*.

The *Best Master Clock* algorithm evaluates the following criteria for each participating device:
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*
- *Clock identity*

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.

4.5.3 Enabling the 802.1AS function

The *802.1AS* function and the *PTP* function cannot be enabled simultaneously on the device.

In the default setting, the *802.1AS* function is disabled. Enabling the *802.1AS* function lets time-aware devices within the same *PTP domain* synchronize.

Perform the following steps on each device within the same *PTP domain*:

- ☐ Open the *Time* > *802.1AS* > *Global* dialog.
- ☐ Enable the *802.1AS* function globally.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Time* > *802.1AS* > *Port* dialog.
- ☐ Enable the *802.1AS* function for *Instance 0*.
  Select the *Instance 0* tab.
  Select the *On* radio button in the *Operation* frame.
- ☐ Enable the *802.1AS* function on the interface.
  In the *Active* column of the desired interface, 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.
`dot1as operation enable`	To enable the *802.1AS* function globally.
`dot1as instance 0 operation enable`	To enable the *802.1AS* function for *Instance 0*.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`dot1as instance 0 operation enable`	To enable the *802.1AS* function on interface `1/1` for *Instance 0*.
`show dot1as data-port-set instance 0 port 1/1`	To check the status of *Instance 0* on interface `1/1`.
`show dot1as current instance 0`	To check the status of *Instance 0*.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 103.

4.5.4 Disabling the 802.1AS function globally

When disabling the *802.1AS* function globally, you disable time synchronization for both instances and for the respective ports allocated to them. This disables time synchronization on the instance and port levels even if the *802.1AS* function is enabled on the instances and on the individual ports.

Perform the following steps on each device within the same *PTP domain*:

- ☐ Open the *Time > 802.1AS > Global* dialog.
- ☐ Disable the *802.1AS* function globally.
  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.
`dot1as operation disable`	To disable the *802.1AS* function globally.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 103.

4.5.5 Disabling the 802.1AS function for an instance

You disable the *802.1AS* function on an instance, for example, in the following situations:
- to disable time synchronization for the ports allocated to the respective instance in one go
- to reallocate a port from one instance to another instance
- to reduce the network load generated by the transmission of synchronization messages

Perform the following steps:

- ☐ Open the *Time > 802.1AS > Port* dialog.
- ☐ Disable the *802.1AS* function for *Instance 0*.
  Select the *Instance 0* tab.
  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.
`dot1as instance 0 operation disable`	To disable the *802.1AS* function for *Instance 0*.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 103.

4.5.6 Disabling the 802.1AS function on a port

You disable the *802.1AS* function on an individual port, for example, in the following situations:
- When the port is connected to a device that is not time-aware and, therefore, does not require time synchronization.
- When you allocate the port to another instance. Before you allocate a port to another instance, we recommend you disable the *802.1AS* function on the port.

Perform the following steps:

- ☐ Open the *Time* > *802.1AS* > *Port* dialog.
  Select the *Instance 0* tab.
- ☐ Deactivate the *802.1AS* function on interface `1/1`.
  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.
`interface 1/1`	To change to the Interface Configuration mode of interface `1/1`.
`dot1as instance 0 operation disable`	To disable the *802.1AS* function on interface `1/1` for *Instance 0*.
`exit`	To change to the Configuration mode.
`exit`	To change to the Privileged EXEC mode.

To save the settings permanently, see section “Saving a configuration profile” on page 103.

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 usb`	To enable the function. When you save a configuration profile, the device saves a copy in the external memory (*ENVM*). `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 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
------ ----------- ----------- ----------- ---------------
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 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 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

Perform the following steps:

- ☐ To change to System Monitor 1, proceed as described in chapter “Access to device management” on page 39.
- ☐ 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 10.3.03. 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 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 `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

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.

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 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
- 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 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.

8.3 Disabling HTTP

The web server provides the Graphical User Interface with the protocol HTTP or HTTPS. HTTPS connections are encrypted, while HTTP connections are unencrypted.

The HTTP protocol is enabled by default. If you disable HTTP, then no unencrypted access to the Graphical User Interface is possible. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *HTTP* tab.
- ☐ 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.

8.4 Disabling Telnet

The device lets you remotely access the device management using Telnet or SSH. Telnet connections are unencrypted, while SSH connections are encrypted.

The Telnet server is enabled in the device by default. If you disable Telnet, then unencrypted remote access to the Command Line Interface is no longer possible. To do this, perform the following steps:

- ☐ Open the *Device Security > Management Access > Server* dialog, *Telnet* tab.
- ☐ 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.

8.5 Disabling the HiDiscovery access

HiDiscovery lets you assign IP parameters to the device over the network during commissioning. HiDiscovery communicates in the device management VLAN without encryption and authentication.

After the device is commissioned, we recommend to set HiDiscovery to read-only or to disable HiDiscovery access completely. To do this, perform the following steps:

- ☐ Open the *Basic Settings > Network > Global* dialog.
- ☐ To take away write permission from the HiDiscovery software, in the *HiDiscovery protocol v1/v2* frame, specify the value *readOnly* in the *Access* field.
- ☐ 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.

8.6 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.

8.6.1 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.

8.7 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

8.8 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 136
- "Transferring an externally generated private RSA key to the device" on page 137

8.8.1 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.

8.8.2 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 137.
- 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 138.

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.

8.9 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 103.

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 103.

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 103.

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 103.

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 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.

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 IP 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)
- Source or destination port of a data packet (IPv4)

You can specify the following ACL types:
- IP ACLs for VLANs
- IP ACLs for ports
- MAC ACLs for VLANs
- MAC ACLs for ports

When you assign both an IP ACL and MAC ACL to the same 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 392.

Note:
You can assign a single ACL to any number of ports or VLANs.

The *ACL* menu contains the following dialogs:
- *IPv4 Rule*
- *MAC Rule*
- *Assignment*

These dialogs provide the following options:
- To specify the rules for the various ACL types.
- To provide the rules with the required priorities.
- To assign the ACLs to ports or VLANs.

9.2.1 Creating and editing IPv4 rules

When filtering IPv4 data packets, the device lets you:
- 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 > 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.).

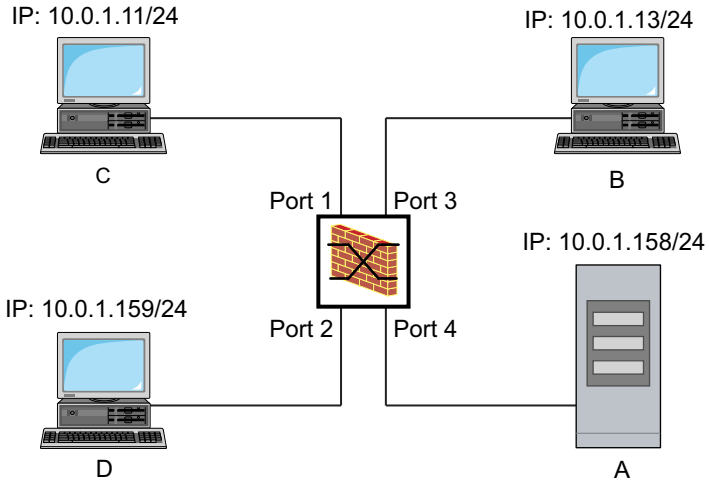


Figure 17: Application example of an IP ACL

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 ACL using the group name.

Perform the following steps:

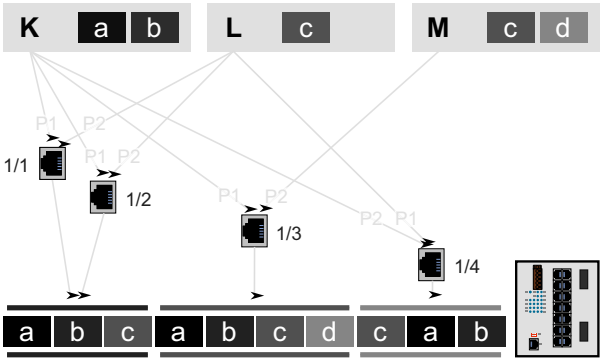
- ☐ Open the *Network Security > ACL > Assignment* dialog.
- ☐ Click the button.
  The dialog displays the *Create* window.
  - ☐ In the *Port/VLAN* field, specify the desired port or the desired VLAN.
  - ☐ In the *Priority* field, specify the priority.
  - ☐ In the *Direction* field, specify the data 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 50 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.

10 Network load control

The device features a number of functions that can help you reduce the network load:
- Direct packet distribution
- Multicasts
- Rate limiter
- Prioritization - QoS
- Flow control

10.1 Direct packet distribution

The device reduces the network load with direct packet distribution.

On each of its ports, the device learns the sender MAC address of received data packets. The device stores the combination “port and MAC address” in its MAC address table (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.

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”).

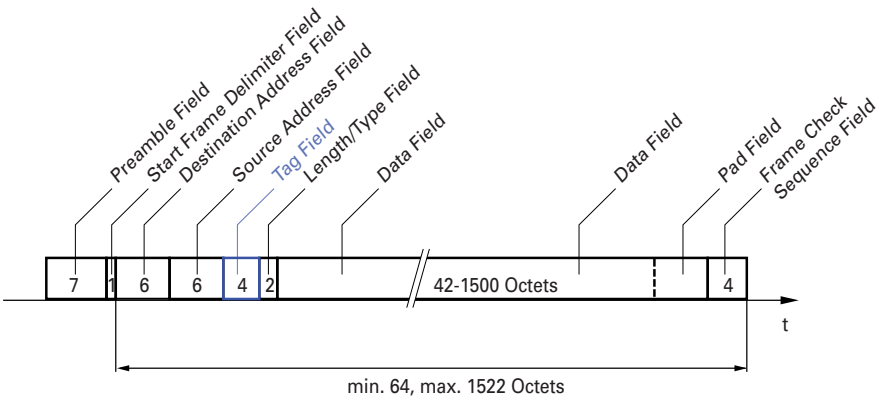


Figure 18: Ethernet data packet with tag

For data packets with VLAN tags, the device evaluates the following information:
- Priority information
- When VLANs are set up, VLAN tagging

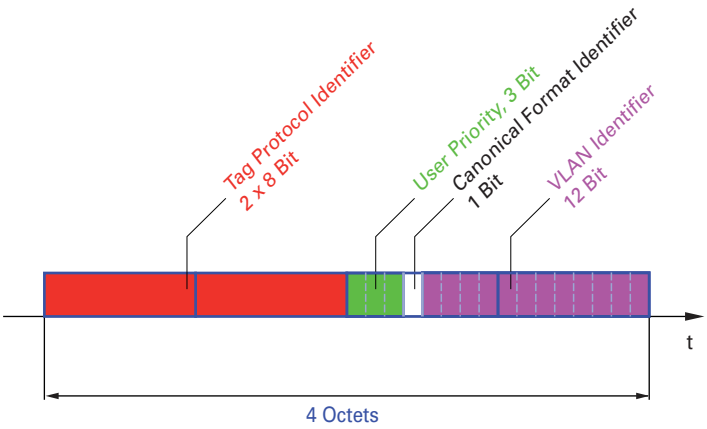


Figure 19: Structure of the VLAN tagging

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.

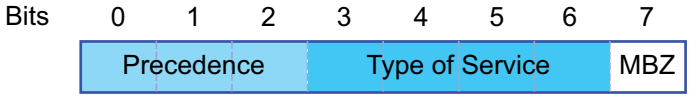


Table 20: ToS field in the IP header

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`	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`.
`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 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.
- In half-duplex mode, the device simulates a collision.

The following figure displays how flow control works. Workstations 1, 2, and 3 want to simultaneously transmit a large amount of data to Workstation 4. The combined bandwidth of Workstations 1, 2, and 3 is greater than the bandwidth of Workstation 4. This causes an overflow on the receive queue of port 4. The left funnel symbolizes this status.

When the flow control function on ports 1, 2 and 3 of the device is enabled, the device reacts before the funnel overflows. The funnel on the right illustrates ports 1, 2 and 3 sending a message to the transmitting devices to control the transmition speed. This results in the receiving port no longer being overwhelmed and is able to process the incoming data packets.

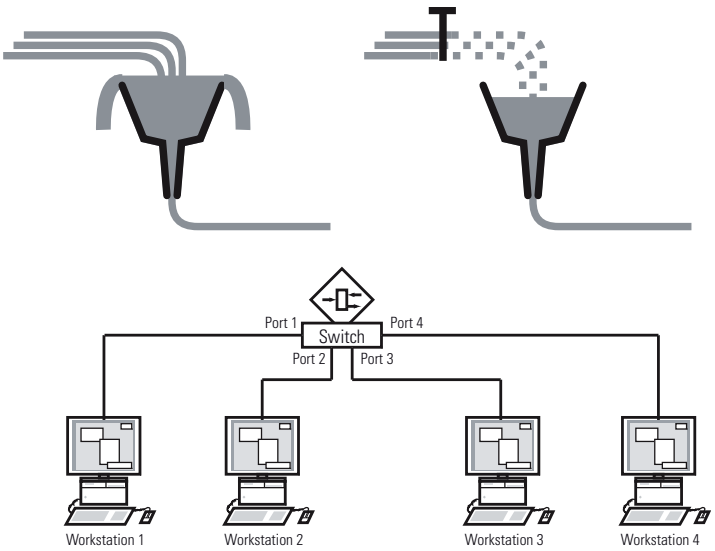


Figure 20: Example of flow control

10.5.1 Flow Control with a half-duplex link

In the example, there is a half-duplex link between Workstation 2 and the device.

Before the send queue of port 2 overflows, the device sends data back to Workstation 2. Workstation 2 detects a collision and stops transmitting.

10.5.2 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.

10.5.3 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 Configuring template-based TSN

11.1 Underlying facts

When you use the *TSN* function, the following basic conditions apply:

- The device operates using the *Store and Forward* method. Thus, the device has to receive the complete data packet before it makes a forwarding decision.
- You specify the Base time and Cycle time once in the device. Both settings are valid for each port participating in TSN.
- You set up a Gate Control List per port based on predefined templates for easier setup.
- Verify that the sum of the Gate Control List entry times is less than or equal to the specified Cycle time.
- The device uses a guard band to help protect the time slot for high priority packets from packets that "leak" from the previous time slot. The decisive factor for the interval length of the guard band is the port speed of the sending port.
  We recommend the following interval lengths for the guard band. The values are based on the port speed and the maximum allowed size of Ethernet packets:
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- The Cycle time range is 50000..10000000 ns.
- The Gate Control List interval range is 1000..10000000 ns.
- Verify that the Cycle time as well as the Gate Control List intervals are multiples of 1 µs, 2 µs or 4 µs.

Table 21: Dependency between Cycle time and granularity

Cycle time	Granularity
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Application example for template-based TSN

This example describes how to set up the devices for a scenario with the following conditions:
- Cycle time = 1 ms
- Time slot for high priority packets = 500 µs
- Time slot for low-priority packets = 487 µs

In this example, each device is connected to the network with a port speed of 1 Gbit/s.

Table 22: Structure of the cycle

Time slot	Traffic classes	Duration
High priority packets	7	500 µs
Low-priority packets	0,1,2,3,4,5,6	487 µs
Guard band	–	13 µs

11.2.1 Time calculation

The device automatically calculates the duration of the time slot for low-priority packets. The calculation is based on the following parameters:
- Cycle time
- Duration of the time slot for high priority packets
- Duration of the guard band

11.2.2 Setting up the devices

Using the previously specified times, you set up the devices using the Graphical User Interface or the Command Line Interface. For each device involved, perform the following steps.

Checking and adjusting the Cycle time

Perform the following steps:

- ☐ Open the *Switching > TSN > Configuration* dialog.
- ☐ Check in the *Configuration* frame the value in the *Cycle time [ns]* field.
- ☐ If necessary, adjust the value.



- ☐ 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.
show tsn configuration
Port  Status                Conf. cycle time[ns]  Conf. base time
      Default gate states   Curr. cycle time[ns]  Curr. base time
      Config change pending                       Time of last activation
----  --------------------  --------------------  ----------------------------
 1/1  [x]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                    1000000  1970-01-01 00:00:00.000000000
      [ ]                                         2018-07-12 08:10:58.813000000

 1/2  [x]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                    1000000  1970-01-01 00:00:00.000000000
      [ ]                                         2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                          0  1970-01-01 00:00:00.000000000
      [ ]                                         1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled             1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                          0  1970-01-01 00:00:00.000000000
      [ ]                                         1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                          If necessary, adjust the value.
```

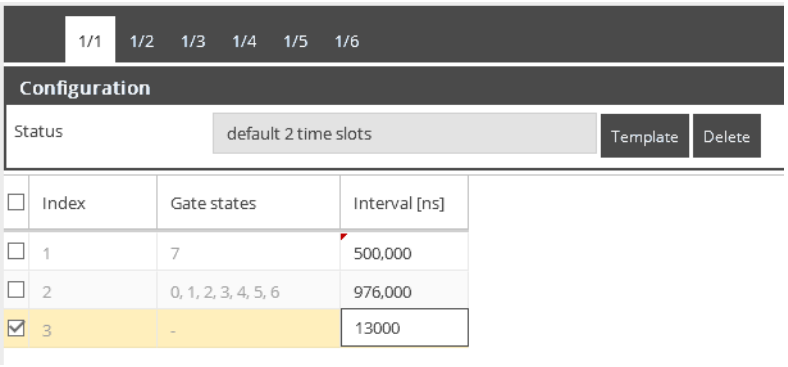
Selecting a template and setting up the Gate Control List

The device provides predefined templates to help you set up the Gate Control List. The following example guides you through the necessary steps using the template *default 2 time slots*. After you select the template, you can adjust the duration of the time slots. Perform the following steps for each port for which you want to use the *TSN* function.

Perform the following steps:

- ☐ Open the *Switching > TSN > Gate Control List > Configured* dialog.
- ☐ Select the tab for the port for which you want to specify the settings.

- ☐ Select a template in the *Configuration* frame.
  Perform the following steps:
  - ☐ Click the *Template* button.
  - ☐ Select the *default 2 time slots* item.
  - ☐ Click the *Ok* button.
- ☐ Adjust the values in the *Interval [ns]* column:
  - ☐ Enter the value `500000` in the row for high priority packets.
  - ☐ Enter the value `13000` in the row for the guard band.
  - ☐ The device calculates the third value automatically when saving the changes.



- ☐ 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`.
`tsn gcl modify 1 interval 500000`	To adjust the duration in nanoseconds of the time slot for high priority packets.
`tsn gcl modify 3 interval 13000`	To adjust the duration in nanoseconds of the time slot for the guard band. The device automatically calculates the duration of the time slot for low-priority packets. You cannot set the time slot for low-priority packets.

12 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.

12.1 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.

12.1.1 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.

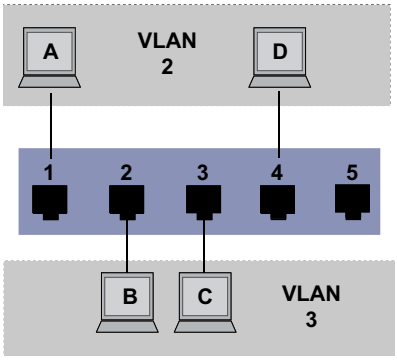


Figure 21: Example of a simple port-based VLAN

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 23: Ingress table

Terminal	Port	Port VLAN identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Table 24: 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............................. 128
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
```

12.1.2 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).

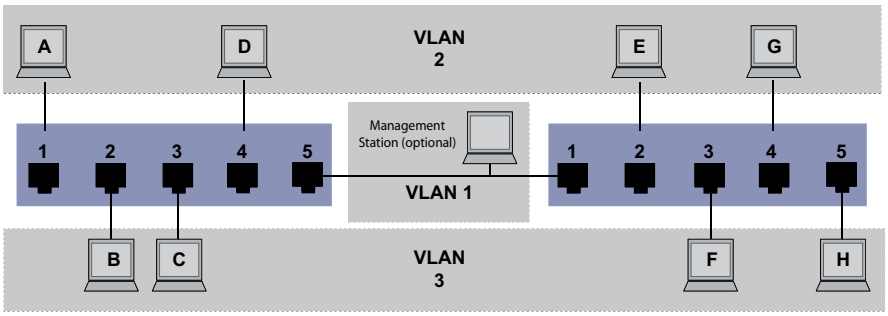


Figure 22: Example of a more complex VLAN configuration

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 25: 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 26: 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 27: 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 28: 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............................. 128
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
```

12.2 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.

12.3 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.

12.4 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.

13 Redundancy

13.1 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

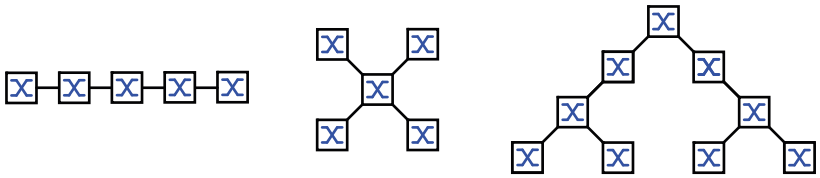


Figure 23: Network with line, star and tree topologies

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.

13.1.1 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.

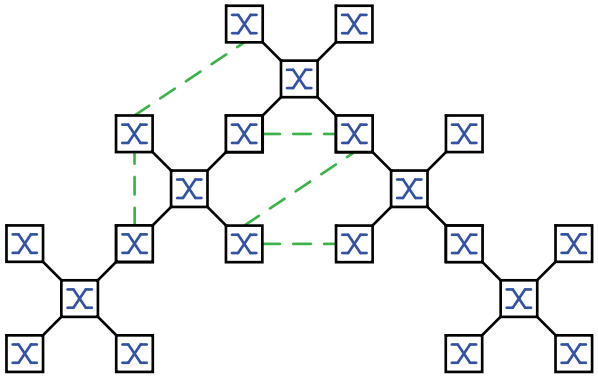


Figure 24: Meshed topology: Tree topology with physical loops

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.

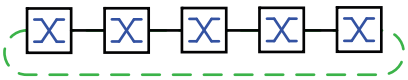


Figure 25: Ring topology: Line topology with connected ends

For operating in this network topology, the device provides you with the following redundancy protocols:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree Protocol (RSTP)

13.1.2 Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

Table 29: 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.
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.

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.

13.1.3 Combinations of redundancy protocols

Table 30: Overview of redundancy protocol combinations

	MRP	RSTP	Link Aggreg.	Link Backup	HIPER Ring
MRP	▲	—	—	—	—
RSTP	▲ 1)	▲	—	—	—
Link Aggreg.	—	▲ 2)	▲	—	—
Link Backup	▲	▲	▲	▲	—
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲

▲ Combination applicable

○ Combination not applicable

1) A redundant coupling between these network topologies will possibly lead to loops.

2) Combination applicable on the same port

13.2 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.

13.2.1 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.

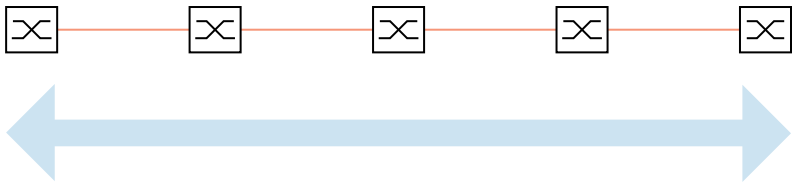


Figure 26: Line structure

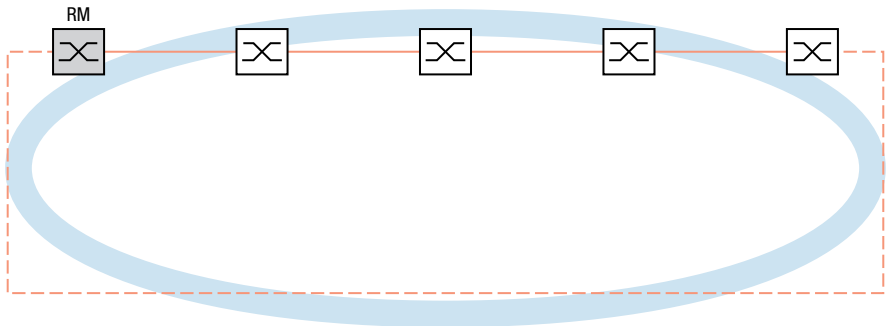


Figure 27: Redundant ring structure
RM = Ring Manager
—— main line
- - - redundant line

13.2.2 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.

13.2.3 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.

13.2.4 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).

13.2.5 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 31: 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.

13.2.6 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.

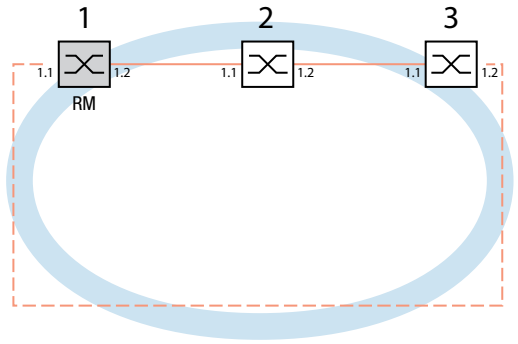


Figure 28: Example of MRP Ring
RM = Ring Manager
—— main line
- - - redundant line

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.

13.3 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.

13.3.1 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.

13.3.2 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 32: 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 209.

13.4 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).

13.4.1 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*.

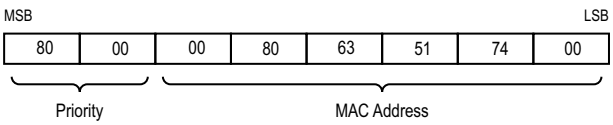


Figure 29: Bridge Identifier, Example (interpretation according to IEEE 802.1D-1998, values in hexadecimal notation)

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 33 on page 214). 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*.

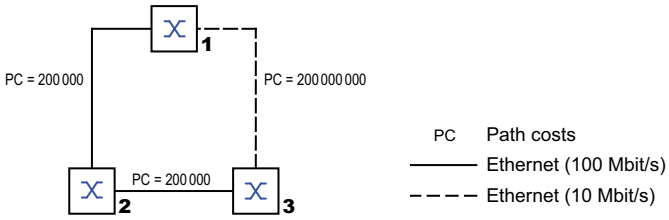


Figure 30: Path costs

Table 33: 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).

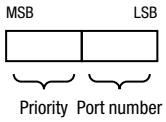


Figure 31: Port Identifier (interpretation according to IEEE 802.1D-1998)

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.

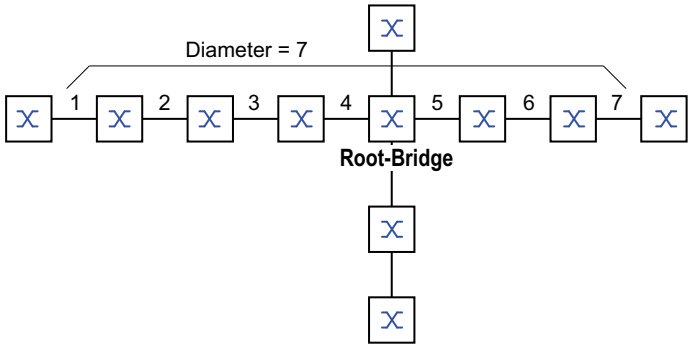


Figure 32: Definition of diameter

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.

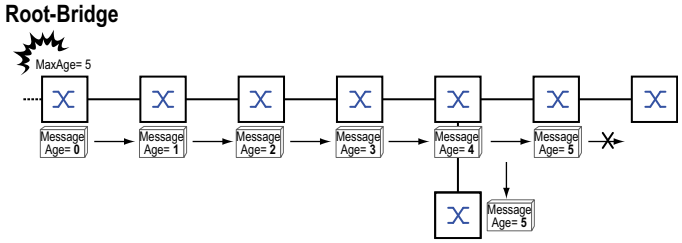


Figure 33: Transmission of an STP-BPDU depending on MaxAge

13.4.2 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 31 on page 215). 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.

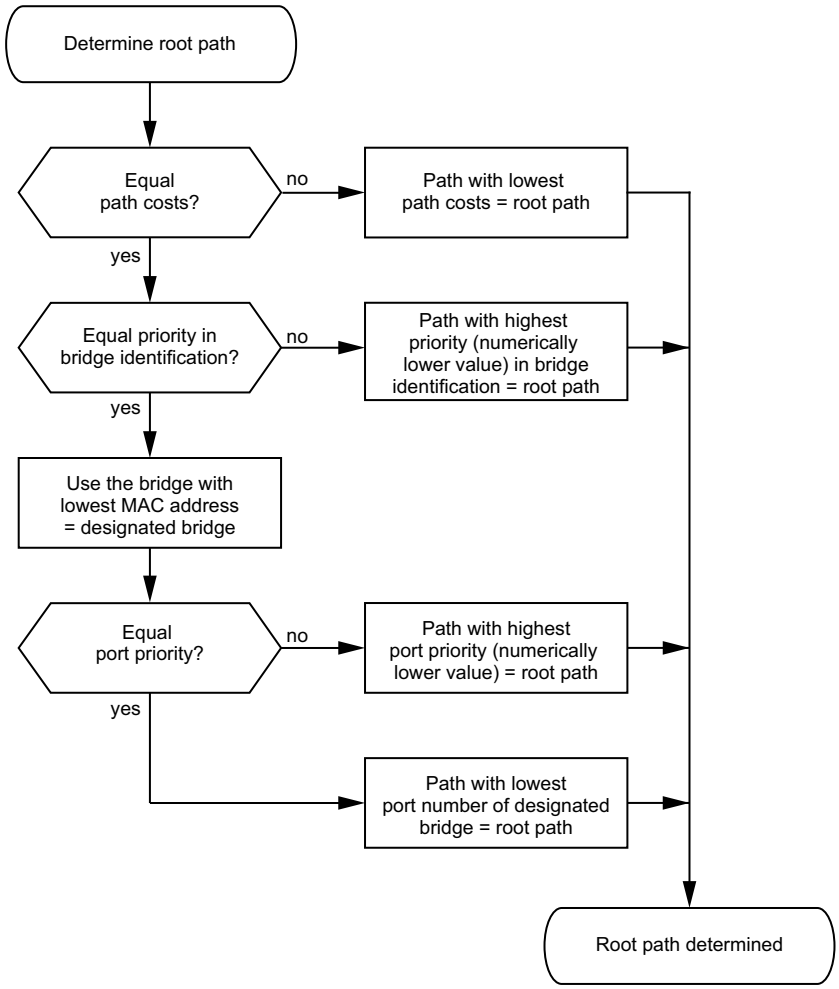


Figure 34: Flow diagram for specifying the root path

13.4.3 Examples

Example of determining the root path

You can use the network plan to follow the flow chart (see figure 34 on page 217) 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).

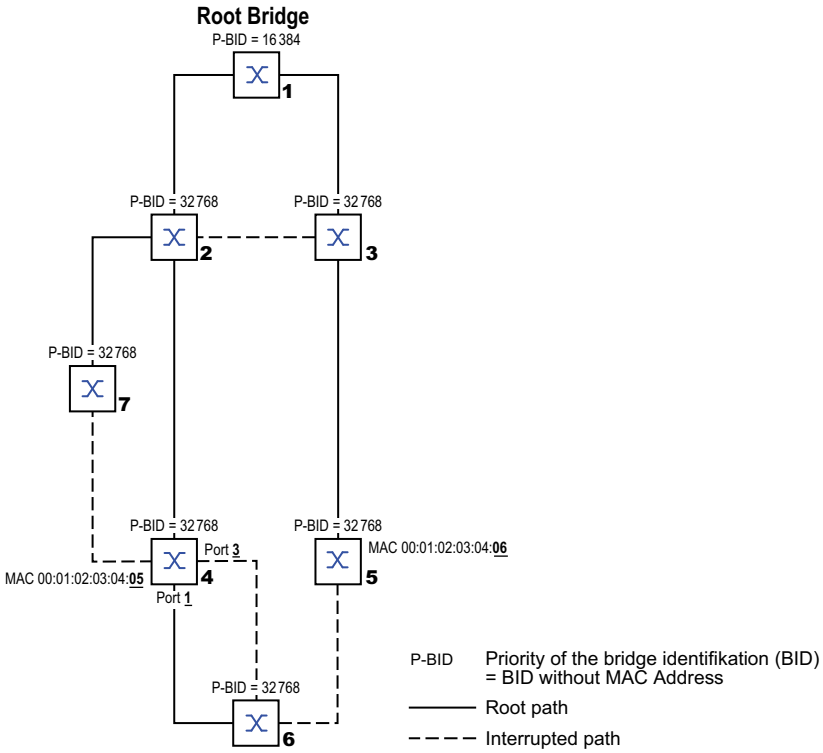


Figure 35: Example of a network plan for determining the root path

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 34 on page 217) 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.

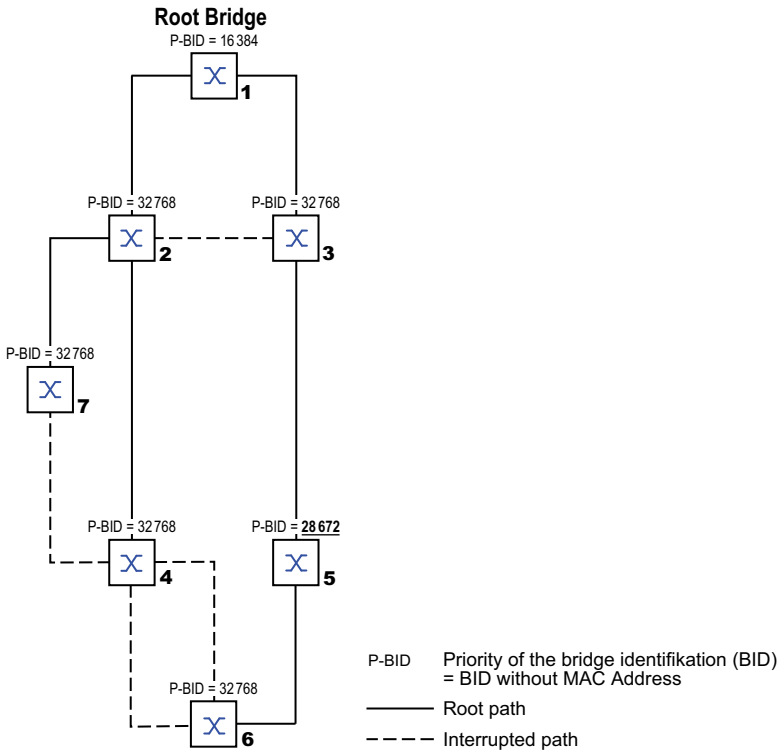


Figure 36: Example of a network plan for manipulating the root path

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.

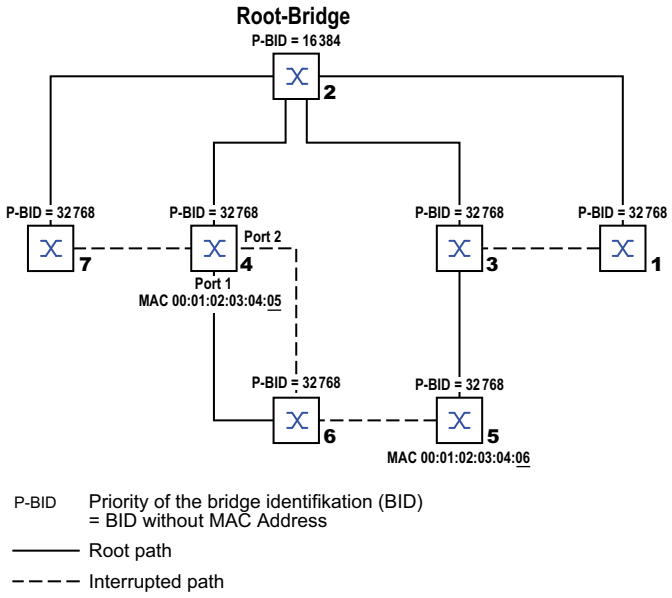


Figure 37: Example of manipulating the tree structure

13.5 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.

13.5.1 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 34 on page 217.
  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.

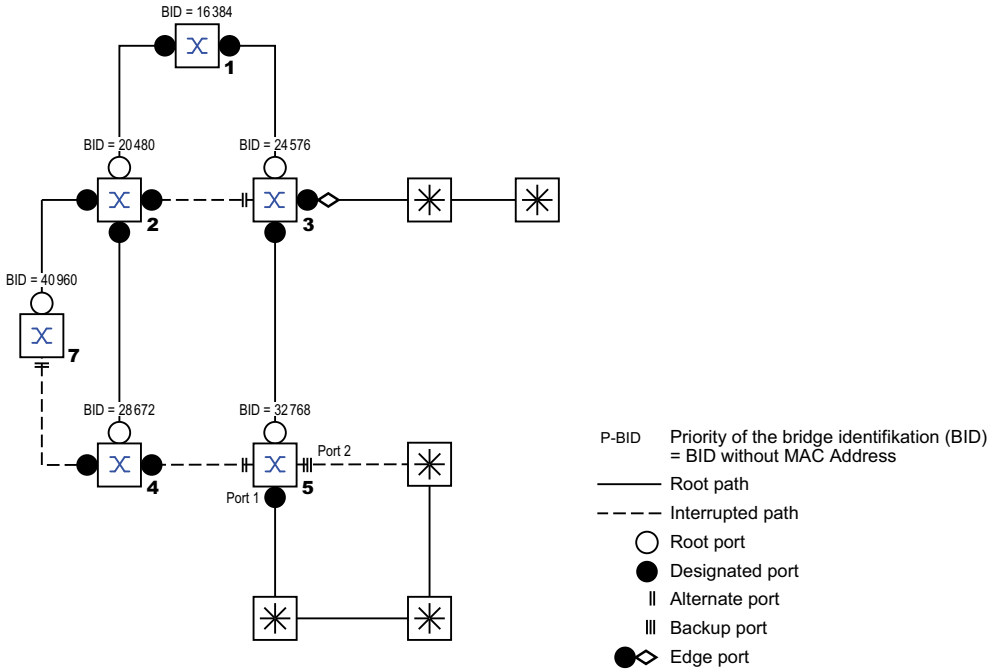


Figure 38: Port role assignment

13.5.2 Port states

Depending on the tree structure and the state of the selected connection paths, RSTP assigns the ports their states.

Table 34: 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)

13.5.3 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.

13.5.4 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.

13.5.5 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:

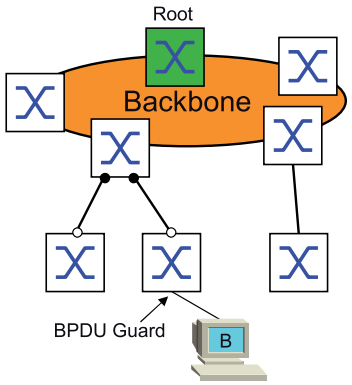
`show spanning-tree global`	To display the parameters for checking.

13.5.6 Guards

The device lets you activate various protection functions (guards) on the ports.

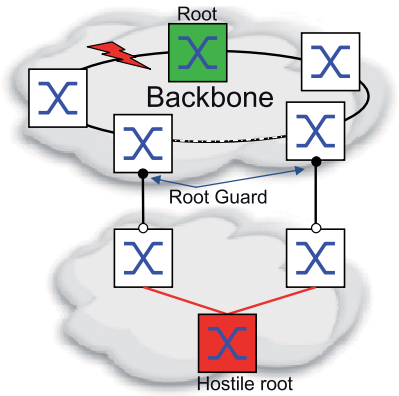
The following protection functions help protect the network from incorrect configurations, loops and attacks with STP-BPDUs:

- *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.

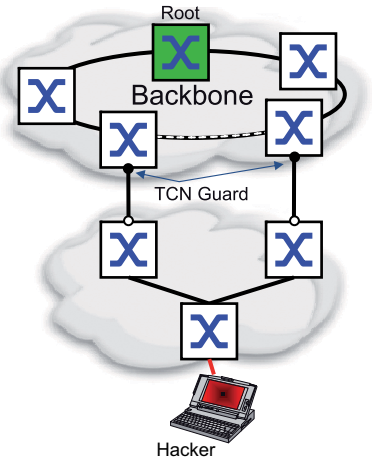
- *Root guard* – for *Designated ports*
  You activate this protection function separately for every port.



  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`.

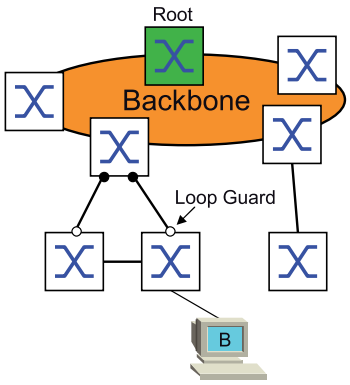
  When there are no STP-BPDUs with better path information to the *Root bridge*, after 2 × *Hello time [s]* the device resets the state of the port to a value according to the port role.

- *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.

13.6 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`.

13.6.1 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 2 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.

13.6.2 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.

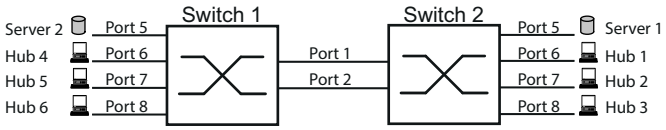


Figure 39: Link Aggregation Switch to Switch Network

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.

13.7 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.

13.7.1 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.

13.7.2 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.

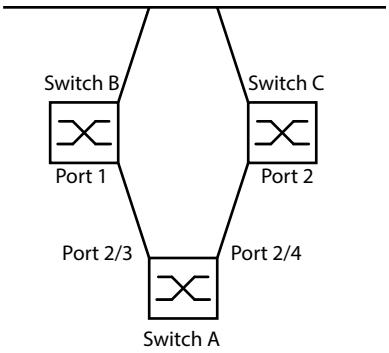


Figure 40: Link Backup example network

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.

14 Operation diagnosis

The device provides you with the following diagnostic tools:
- Sending SNMP traps
- Monitoring the Device Status
- Event counter at port level
- Detecting non-matching duplex modes
- Auto-Disable
- Topology discovery
- Detecting IP address conflicts
- Detecting 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
- *Basic Settings > Power over Ethernet > Global* dialog **(depends on hardware)**
- *Network Security > Port Security* dialog
- *Switching > L2-Redundancy > Link Aggregation* dialog
- *Diagnostics > Status Configuration > Device Status* dialog
- *Diagnostics > Status Configuration > Security Status* dialog
- *Diagnostics > Status Configuration > 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:
- 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.

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 35: 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.
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.

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*.

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:
- 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 36: 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.
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.

Table 36: Security Status events (cont.)

Name	Meaning
IEC 61850/MMS active	The device monitors the IEC 61850/MMS protocol activation setting.
Self-signed HTTPS certificate present	The device monitors the HTTPS server for self-generated digital certificates.
Modbus TCP active	The device monitors the Modbus TCP/IP protocol activation setting.

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 monitor iec61850-mms-enabled`	To monitor the *IEC 61850/MMS* function. When you enable the *IEC 61850/MMS* function, the value in the *Security status* frame changes to *error*.
`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 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 37: 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.

14.4.1 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:

- Duplex problem detected
  Mismatched duplex modes.

- EMI
  Electromagnetic interference.
- Network extension
  The network extension is too great, or too many cascading hubs.
- Collisions, *Late Collisions*
  In half-duplex mode, collisions mean normal operation.
  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 38: 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
1	marked	Half-duplex	None	OK	
2	marked	Half-duplex	Collisions	OK	
3	marked	Half-duplex	Late Collisions	Duplex problem detected	Potential duplex problem, EMI, network extension
4	marked	Half-duplex	CRC Error	OK	EMI
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
9	unmarked	Half-duplex	None	OK	
10	unmarked	Half-duplex	Collisions	OK	
11	unmarked	Half-duplex	Late Collisions	Duplex problem detected	Potential duplex problem, EMI, network extension
12	unmarked	Half-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

14.5 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)
- *Spanning Tree*
- *Port Security*
- *Overload detection* (*Port Monitor* function)
- *Link speed/Duplex mode detection* (*Port Monitor* function)

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.

14.6 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.

14.6.1 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.

14.6.2 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

14.7 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.

14.8 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.

14.8.1 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.

14.8.2 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 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 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
```

14.8.3 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.

14.8.4 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

14.9 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.

14.10 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.

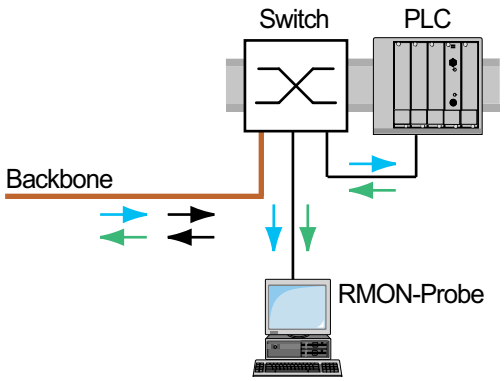


Figure 41: Application example of a port-mirroring setup

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.

14.10.1 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.

14.11 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, set the device to the Recovery Mode, see section "Access to device management" 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
```

14.12 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

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.

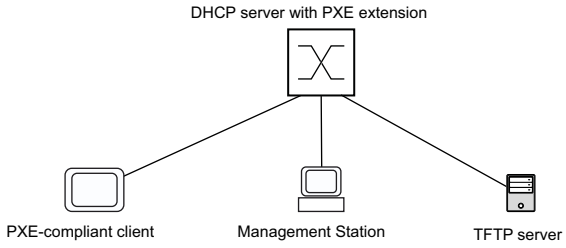


Figure 42: Simple structure of a Preboot eXecution Environment (PXE) setup

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 264 or “Setting up a dynamic pool” on page 265. 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*.

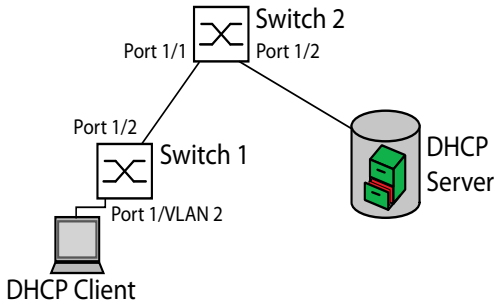


Figure 43: DHCP Layer 2 Example Network

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 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.

15.3.1 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.

15.3.2 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.

15.4 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.

15.4.1 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.

15.4.2 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.

15.4.3 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.

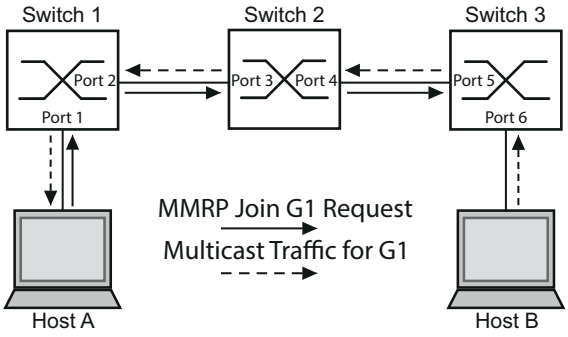


Figure 44: MMRP Network for MAC address Registration

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.

15.4.4 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.

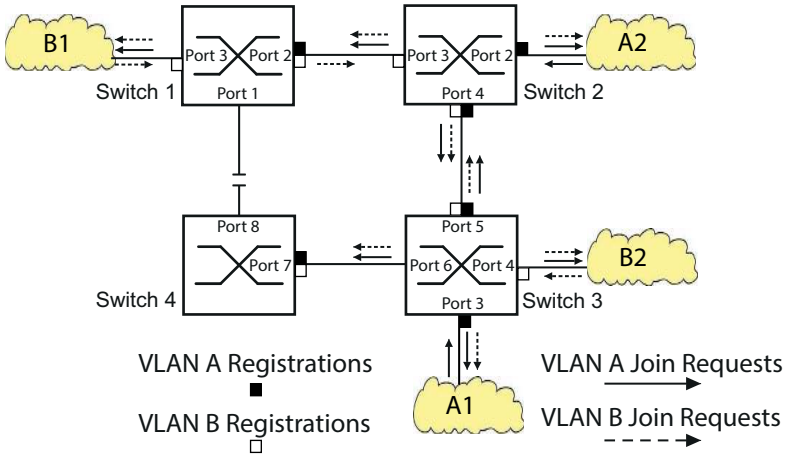


Figure 45: MVRP Example Network for VLAN Registration

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.

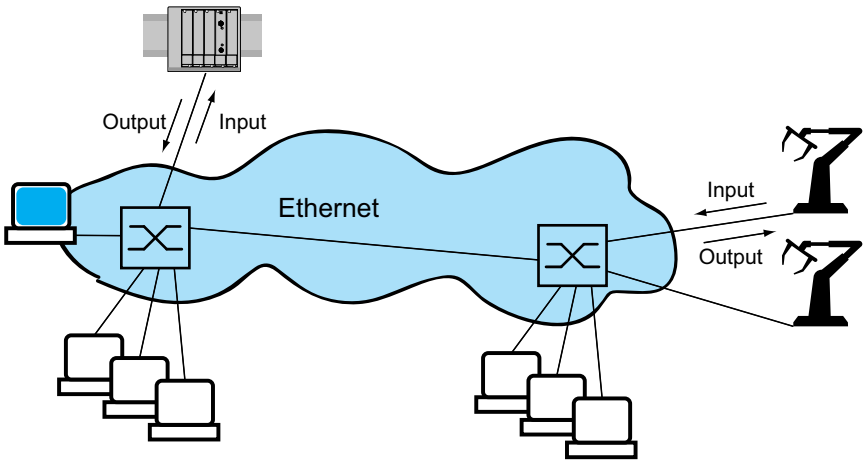


Figure 46: Example of communication.

16.1 IEC 61850/MMS

IEC 61850/MMS is an industrial communication protocol standardized by the International Electrotechnical Commission (IEC). The protocol is to be found in substation automation, for example in the control technology of energy suppliers.

This protocol, which works in a packet-oriented way, is based on the TCP/IP transport protocol and uses the Manufacturing Messaging Specification (MMS) for the client-server communication. The protocol is object-oriented and defines a standardized configuration language that comprises, among other things, functions for SCADA, Intelligent Electronic Devices (IED) and for the network control technology.

Part 6 of the IEC 61850 standard defines the configuration language SCL (Substation Configuration Language). SCL describes the properties of the device and the system structure in an automatically processable form. The properties of the device described with SCL are stored in the ICD file in the device.

16.1.1 Switch model for IEC 61850

The Technical Report, IEC 61850 90-4, specifies a bridge model. The bridge model represents the functions of a switch as objects of an Intelligent Electronic Device (IED). An MMS client (for example the control room software) uses these objects to monitor and set up the device.

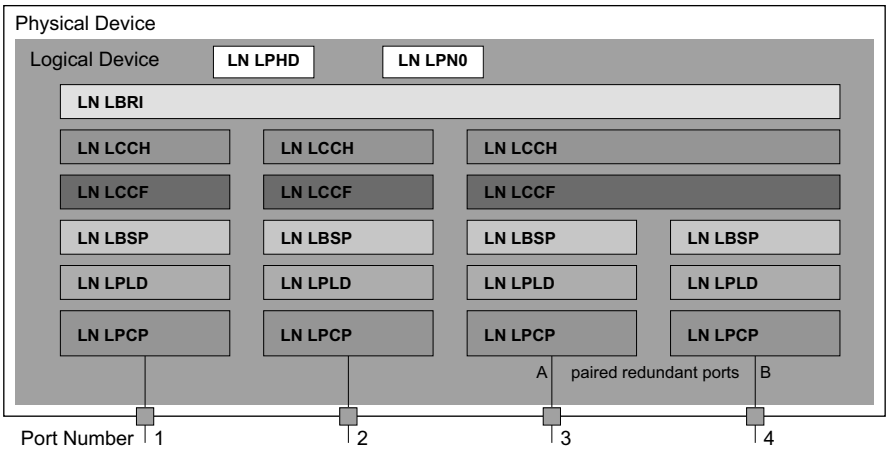


Figure 47: Bridge model based on Technical Report IEC 61850 90-4

Table 39: Classes of the bridge model based on TR IEC 61850 90-4

Class	Description
LN LLN0	Zero logical node of the Bridge IED: Defines the logical properties of the device.
LN LPHD	Physical Device logical node of the Bridge IED: Defines the physical properties of the device.
LN LBRI	Bridge logical node: Represents general settings of the bridge functions of the device.
LN LCCH	Communication Channel logical node: Defines the logical Communication Channel that consists of one or more physical ports.

Table 39: Classes of the bridge model based on TR IEC 61850 90-4 (cont.)

Class	Description
LN LCCF	Channel Communication Filtering logical node: Defines the VLAN and Multicast settings for the higher-level Communication Channel.
LN LBSP	Port Spanning Tree Protocol logical node: Defines the Spanning Tree statuses and settings for the respective physical port.
LN LPLD	Port Layer Discovery logical node: Defines the LLDP statuses and settings for the respective physical port.
LN LPCP	Physical Communication Port logical node: Represents the respective physical port.

16.1.2 Integration into a Control System

Preparation of the device

Perform the following steps:

- ☐ Check that the device has an IP address assigned.
- ☐ Open the *Advanced > Industrial Protocols > IEC 61850/MMS* dialog.
- ☐ Start the MMS server.

  Select the *On* radio button in the *Operation* frame and click the  button.
  Afterwards, an MMS client is able to connect to the device and to read and monitor the objects defined in the bridge model.

IEC 61850/MMS does not provide any authentication mechanisms. If the write access for IEC 61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. As a result, incorrect device settings and potential network interruptions may occur.

NOTICE

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

☐ To allow the MMS client to change the settings, mark the *Write access* checkbox, and click the button.

Offline configuration

The device lets you download the ICD file using the Graphical User Interface. This file contains the properties of the device described with SCL and lets you set up the substation without directly connecting to the device.

☐ Open the *Advanced > Industrial Protocols > IEC 61850/MMS* dialog.

☐ To load the ICD file to your PC, click the button.

Monitoring the device

The IEC 61850/MMS server integrated into the device lets you monitor multiple statuses of the device by means of the Report Control Block (RCB). Up to 5 MMS clients can register for a Report Control Block at the same time.

The device lets you monitor the following statuses:

Table 40: Statuses of the device that can be monitored with IEC 61850/MMS

Class	RCB object	Description
LN LPHD	TmpAlm	When the temperature measured in the device exceeds or falls below the specified temperature threshold values, the status changes.
	PhyHealth	When the status of the LPHD.TmpAlm RCB object changes, the status changes.
LN LPHD	TmpAlm	When the temperature measured in the device exceeds or falls below the specified temperature threshold values, the status changes.
	PhyHealth	When the status of the LPHD.PwrSupAlm or LPHD.TmpAlm RCB object changes, the status changes.

Table 40: Statuses of the device that can be monitored with IEC 61850/MMS (cont.)

Class	RCB object	Description
LN LBRI	RstpRoot	When the device takes over or relinquishes the role of the *Root bridge*, the status changes.
	RstpTopoCnt	When the topology changes due to a change of the *Root bridge*, the status changes.
LN LCCH	ChLiv	When the link status of the physical port changes, the status changes.
LN LPCP	PhyHealth	When the link status of the physical port changes, the status changes.

16.2 Modbus TCP function

Modbus TCP is an application layer messaging protocol providing client/server communication between the client and devices connected in Ethernet TCP/IP networks.

The *Modbus TCP* function lets you install the device in networks already using *Modbus TCP* and retrieve information saved in the registers in the device.

16.2.1 Client/Server Modbus TCP/IP Mode

The device supports the client/server model of Modbus TCP/IP. This device operates as a server in this constellation and responds to requests from a client for information saved in the registers.

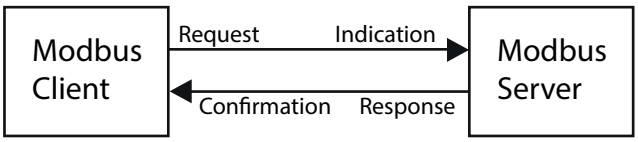


Figure 48: Client/Server Modbus TCP/IP Mode

The client / server model uses four types of messages to exchange data between the client and server:

- Modbus TCP/IP Request, the client generates a request for information and sends it to the server.
- Modbus TCP/IP Indication, the server receives a request as an indication that a client requires information.
- Modbus TCP/IP Response, when the required information is available, the server sends a reply containing the requested information. When the requested information is unavailable, the server sends an Exception Response to notify the client of the error detected during the processing. The Exception Response contains an exception code indicating the reason for the detected error.
- Modbus TCP/IP Confirmation, the client receives a response from the server, containing the requested information.

16.2.2 Supported Functions and Memory Mapping

The device supports functions with the public codes `0x03` (`Read Holding Registers`) and `0x05` (`Write Single Coil`). The codes let you read the information saved in the registers such as the system information, including the system name, system location, software version, IP address, MAC address. The codes also let you read the port information and port statistics. The `0x05` code lets you reset the port counters individually or globally.

The following list contains definitions for the values entered in the `Format` column:

- Bitmap: a group of 32-bits, encoded into the Big-endian byte order and saved in 2 registers. Big-endian systems save the most significant byte of a word in the smallest address and save the least significant byte in the largest address.
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected

- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted-Pair (TP)
  - 2 = Fiber - 10 Mbit/s
  - 3 = Fiber - 100 Mbit/s
  - 4 = Giga - 10/100/1000 Mbit/s (triple speed)
  - 5 = Giga - Copper 1000 Mbit/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- String: octets, saved in sequence, 2 octets per register.

Modbus TCP/IP Codes

The addresses in the following tables allow the client to reset port counters and retrieve specific information from the device registers.

Table 41: System/Global Information

Address	Qty	Description	Min	Max	Step	Unit	Format
0000	128	System Name	-	-	-	-	String
0080	128	System Contact	-	-	-	-	String
0100	128	System Location	-	-	-	-	String
0180	128	Software Version	-	-	-	-	String
0200	32	OrderCode	-	-	-	-	String
0220	16	Serial Number	-	-	-	-	String
0230	1	IP Address[0]	0	254	1	-	F1
0231	1	IP Address[1]	0	254	1	-	F1
0232	1	IP Address[2]	0	254	1	-	F1
0233	1	IP Address[3]	0	254	1	-	F1
0234	1	NetMask[0]	0	255	1	-	F1
0235	1	NetMask[1]	0	255	1	-	F1
0236	1	NetMask[2]	0	255	1	-	F1
0237	1	NetMask[3]	0	255	1	-	F1
0238	1	GateWay[0]	0	254	1	-	F1
0239	1	GateWay[1]	0	254	1	-	F1
023A	1	GateWay[2]	0	254	1	-	F1
023B	1	GateWay[3]	0	254	1	-	F1
023C	3	MacAddress	-	-	-	-	String
023F	1	PowerAlarm1	0	1	1	-	F2
0240	1	PowerAlarm2	0	1	1	-	F2
0241	1	StpState	0	1	1	-	F1
0242	2	Number of Ports	1	64	1	-	F1
0244	1	Reset Counter (all Counter)	0	1	1	-	F1
0245	4	Port Present Map	-	-	-	-	Bitmap
0249	4	Port Link Map	-	-	-	-	Bitmap
024D	4	Port Stp State Map	-	-	-	-	Bitmap
0251	4	Port Activity Map	-	-	-	-	Bitmap

Table 42: Port Information

Address	Qty	Description	Min	Max	Step	Unit	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Table 43: Port Statistics

Address	Qty	Description	Min	Max	Step	Unit	Format
0800	2	Port1 - Number of bytes received	0	4294967295 (2^{32}-1)	1	-	F9
0802	2	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	2	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	2	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	2	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	2	Port1 - Total frames received	0	4294967295	1	-	F9
080C	2	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	2	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	2	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	2	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	2	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	2	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	2	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	2	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	2	Port1 - Number of 64-byte frames rcvd/ sent	0	4294967295	1	-	F9
081E	2	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	2	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9

Table 43: Port Statistics (cont.)

Address	Qty	Description	Min	Max	Step	Unit	Format
0822	2	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	2	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	2	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	2	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	2	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	2	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	2	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	2	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
0832	2	Port2 - Number of bytes received	0	4294967295	1	-	F9
0834	2	Port2 - Number of bytes sent	0	4294967295	1	-	F9
0836	2	Port2 - Number of frames received	0	4294967295	1	-	F9
0838	2	Port2 - Number of frames sent	0	4294967295	1	-	F9
083A	2	Port2 - Total bytes received	0	4294967295	1	-	F9
083C	2	Port2 - Total frames received	0	4294967295	1	-	F9
083E	2	Port2 - Number of broadcast frames received	0	4294967295	1	-	F9
0840	2	Port2 - Number of multicast frames received	0	4294967295	1	-	F9
0842	2	Port2 - Number of frames with CRC error	0	4294967295	1	-	F9
0844	2	Port2 - Number of oversized frames received	0	4294967295	1	-	F9
0846	2	Port2 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0848	2	Port2 - Number of jabber frames received	0	4294967295	1	-	F9
084A	2	Port2 - Number of collisions occurred	0	4294967295	1	-	F9
084C	2	Port2 - Number of late collisions occurred	0	4294967295	1	-	F9
084E	2	Port2 - Number of 64-byte frames rcvd/ sent	0	4294967295	1	-	F9
0850	2	Port2 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0852	2	Port2 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0854	2	Port2 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0856	2	Port2 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0858	2	Port2 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
085A	2	Port2 - Number of Mac Error Packets	0	4294967295	1	-	F9
085C	2	Port2 - Number of dropped received packets	0	4294967295	1	-	F9
085E	2	Port2 - Number of multicast frames sent	0	4294967295	1	-	F9
0860	2	Port2 - Number of broadcast frames sent	0	4294967295	1	-	F9
0862	2	Port2 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
144E	2	Port64 - Number of bytes received	0	4294967295	1	-	F9

Table 43: Port Statistics (cont.)

Address	Qty	Description	Min	Max	Step	Unit	Format
1450	2	Port64 - Number of bytes sent	0	4294967295	1	-	F9
1452	2	Port64 - Number of frames received	0	4294967295	1	-	F9
1454	2	Port64 - Number of frames sent	0	4294967295	1	-	F9
1456	2	Port64 - Total bytes received	0	4294967295	1	-	F9
1458	2	Port64 - Total frames received	0	4294967295	1	-	F9
145A	2	Port64 - Number of broadcast frames received	0	4294967295	1	-	F9
145C	2	Port64 - Number of multicast frames received	0	4294967295	1	-	F9
145E	2	Port64 - Number of frames with CRC error	0	4294967295	1	-	F9
1460	2	Port64 - Number of oversized frames received	0	4294967295	1	-	F9
1462	2	Port64 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
1464	2	Port64 - Number of jabber frames received	0	4294967295	1	-	F9
1466	2	Port64 - Number of collisions occurred	0	4294967295	1	-	F9
1468	2	Port64 - Number of late collisions occurred	0	4294967295	1	-	F9
146A	2	Port64 - Number of 64-byte frames rcvd/ sent	0	4294967295	1	-	F9
146C	2	Port64 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
146E	2	Port64 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
1470	2	Port64 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
1472	2	Port64 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
1474	2	Port64 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
1476	2	Port64 - Number of Mac Error Packets	0	4294967295	1	-	F9
1478	2	Port64 - Number of dropped received packets	0	4294967295	1	-	F9
147A	2	Port64 - Number of multicast frames sent	0	4294967295	1	-	F9
147C	2	Port64 - Number of broadcast frames sent	0	4294967295	1	-	F9
147E	2	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 Application example for the Modbus TCP function

In the following example, you set up the device to respond to client requests. The prerequisite for this configuration is that the client device is set up with an IP address within the given range. The *Write access* function remains inactive for this example. When you activate the *Write access* function, the device lets you reset the port counters only. In the default setting the *Modbus TCP* and *Write access* functions are inactive.

The *Modbus TCP* function does not provide any authentication mechanisms. If the write access for *Modbus TCP* is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. As a result, incorrect device settings and potential network interruptions may occur.

NOTICE

RISK OF UNAUTHORIZED ACCESS TO THE DEVICE

Only activate the write access if you have taken additional measures (for example Firewall, VPN, etc.) to reduce possible unauthorized access.

Failure to follow these instructions can result in equipment damage.

Perform the following steps:

- ☐ Open the *Device Security > Management Access > IP Access Restriction* dialog.
- ☐ Add a table row. To do this, click the button.
- ☐ Specify the IP address range in the table row where the *Index* column has the value `2`. To do this, enter the following values:
  - In the *Address* column: `10.17.1.0`
  - In the *Netmask* column: `255.255.255.248`
- ☐ Verify that the checkbox in the *Modbus TCP* column is marked.
- ☐ Activate the IP address range. To do this, mark the checkbox in the *Active* column.
- ☐ Apply the settings temporarily. To do this, click the button.
- ☐ Open the *Diagnostics > Status Configuration > Security Status* dialog, *Global* tab.
- ☐ Verify that the checkbox related to the parameter *Modbus TCP active* is marked.
- ☐ Open the *Advanced > Industrial Protocols > Modbus TCP* dialog.
- ☐ The standard *Modbus TCP* listening port, port `502`, is the default setting. However, when you wish to listen on another TCP port, enter the value for the listening port in the *TCP port* field.
- ☐ Enable the *Modbus TCP* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the button.

When you enable the *Modbus TCP* function, the *Security Status* function detects the activation and displays an alarm in the *Basic Settings > System* dialog, *Security status* frame.

`enable`	To change to the Privileged EXEC mode.
`network management access add 2`	To add the entry for the address range in the network. Number of the next available index in this example: `2`.
`network management access modify 2 ip 10.17.1.0`	To specify the IP address.
`network management access modify 2 mask 29`	To specify the netmask.
`network management access modify 2 modbus-tcp enable`	To specify that the device lets *Modbus TCP* have access to the device management.
`network management access operation`	To enable the IP access restriction.
`configure`	To change to the Configuration mode.
`security-status monitor modbus-tcp-enabled`	To specify that the device monitors the activation of the *Modbus TCP* server.
`modbus-tcp operation`	To enable the *Modbus TCP* server.
`modbus-tcp port <1..65535>`	To specify the TCP port for *Modbus TCP* communication (optionally). The default setting is port `502`.
`show modbus-tcp`	To display the *Modbus TCP* Server settings.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.............enabled
Write-access...............................disabled
Listening port.............................502
Max number of sessions.....................5
Active sessions............................0
```

`show security-status monitor`	To display the security-status settings.

```
Device Security Settings
Monitor
--------------------------------
Password default settings unchanged..........monitored
...
Write access using HiDiscovery is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....................monitored
Modbus TCP/IP server active..................monitored
```

`show security-status event`	To display occurred security status events.

```
Time stamp             Event                       Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)          -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)    -
2014-01-01 23:47:40   modbus-tcp-enabled(23)       -
show network management access rules 1
```

To display the restricted management access rules for index 1.

```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP function

EtherNet/IP is an industrial communication protocol that is deployed worldwide and is maintained by the Open DeviceNet Vendor Association (ODVA). It is based on the protocols *TCP/IP* and *UDP/IP* over Ethernet. *EtherNet/IP* is supported by leading manufacturers, thus providing a wide base for effective data communication in the industry sector.

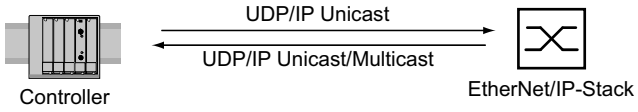


Figure 49: EtherNet/IP network

EtherNet/IP adds the industry protocol CIP (Common Industrial Protocol) to the standard Ethernet protocols. *EtherNet/IP* implements CIP at the Session layer and above and adapts CIP to the specific *EtherNet/IP* technology at the Transport layer and below. In the case of automation applications, *EtherNet/IP* implements CIP on the application level. Therefore, *EtherNet/IP* is ideally suited to the industrial control technology sector.

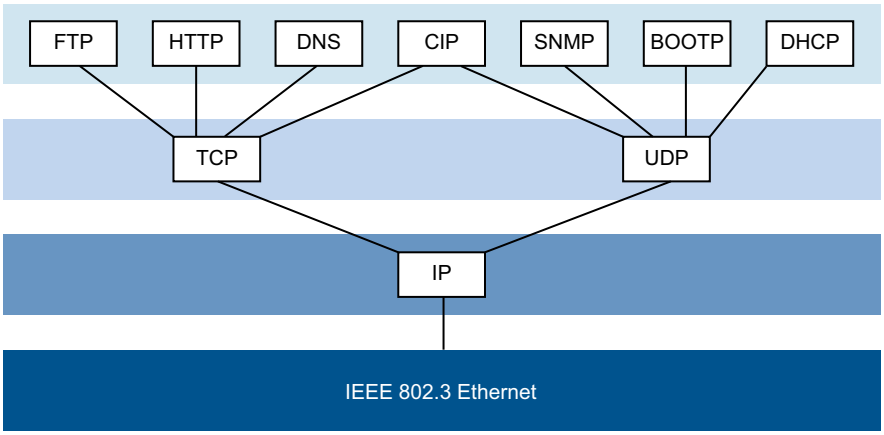


Figure 50: IEEE 802.3 EtherNet/IP

In particular, you find *EtherNet/IP* in the USA and in conjunction with Rockwell controllers.

For further information on EtherNet/IP, see the ODVA website at www.odva.org.

16.3.1 Integration into a Control System

Perform the following steps:

- ☐ Open the *Switching > IGMP Snooping > Global* dialog.
  Verify that the *IGMP Snooping* function is enabled.
- ☐ Open the *Advanced > Industrial Protocols > EtherNet/IP* dialog.
  Verify that the *EtherNet/IP* function is enabled.
- ☐ Open the *Advanced > Industrial Protocols > EtherNet/IP* dialog.
- ☐ To save the EDS as a ZIP archive on your PC, click *Download*.
  The ZIP archive contains the *EtherNet/IP* configuration file and the icon used to set up the controller to connect to the device.

Configuration of a PLC using the example of Rockwell software

Perform the following steps:

- ☐ Open the “EDS Hardware Installation Tool” of RSLinx.
- ☐ Use the “EDS Hardware Installation Tool” to add the EDS file.
- ☐ Restart the “RSLinx” service so that RSLinx takes over the EDS file of the device.
- ☐ Use RSLinx to check if RSLinx has detected the device.
- ☐ Open your Logix 5000 project.
- ☐ Integrate the device into the Ethernet port of the controller as a new module (Generic Ethernet Module).

Table 44: Settings for integrating a Generic Ethernet Module

Setting	I/O connection	Input only	Listen only
Comm Format	Data - DINT	Data - DINT	Input data - DINT - Run/Program
IP address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	2	2	2
Input Size	7	7	7
Output Assembly Instance	1	254	255
Output Size	1	0	0
Configuration Assembly Instance	3	3	3
Configuration Size	0	0	0

- ☐ In the module properties, enter a value of at least 100 ms for the Request Packet Interval (RPI).

Note:
Monitoring the I/O connection to the CPU of the device as a detected failure can result in a potential system failure. Therefore, do not consider the I/O connection to the CPU when monitoring.
The I/O connection between the programmable logic controller (PLC) and the device can be interrupted by a management program. For example, a management station can saturate the CPU of the device with higher priority Real Time (RT) data. In this case, the device can still transmit or receive data packets and the system remains operational.

Example of integration from the Sample Code Library

The Sample Code Library is a website from Rockwell. The object of the website is to provide users with a place where they can exchange their best architecture integration applications.

On the website samplecode.rockwellautomation.com, search for catalog number 9701. This is the catalog number of an example for integrating the Hirschmann device into RS Logix 5000 rel. 16, PLC firmware release 16.

16.3.2 EtherNet/IP Entity Parameters

The following paragraphs identify the objects and operations supported by the device.

Supported operations

Table 45: Overview of the supported EtherNet/IP requests for the objects instances

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Identity object

The device supports the identity object (*Class Code 0x01*) of *EtherNet/IP*. The Hirschmann manufacturer ID is 634. Hirschmann uses the ID 44 (0x2C) to indicate the product type "Managed Ethernet Switch".

Table 46: Instance attributes (only instance 1 is available)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Hirschmann634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type

Table 46: Instance attributes (only instance 1 is available) (cont.)

Id	Attribute	Access Rule	Data type	Description
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (constantly 1) 2: Configured (constantly 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Hirschmann" + product family + product ID + software variant.

TCP/IP Interface Object

The device supports only Instance 1 of the TCP/IP Interface Object (*Class Code 0xF5*) of *EtherNet/IP*.

Depending on the write access status, the device stores the complete settings in its flash memory. Saving the settings can take up to 10 seconds. If the saving process is interrupted for example, due to an inoperable power supply, then the operation of the device might be impossible.

Note:
The device replies to the configuration change `Get Request` with a `Response` although the configuration has not yet been saved completely.

Table 47: Class attributes

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently added: 1

Table 48: Attributes of Instance 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config) 6: ACD status (default 0) 7: ACD fault (default 0)

Table 48: Attributes of Instance 1 (cont.)

Id	Attribute	Access Rule	Data type	Description
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client 1: DNS Client 2: DHCP Client 3: DHCP-DNS Update 4: Configuration setable (within CIP) Other bits reserved (0) 7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3: 4: One device uses DNS for name lookup (constantly 0 because it is unsupported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of: UINT PathSize EPATH Path	Path to the Physical Link Object, constantly {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
0x5	Interface Configuration	Set/Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IP Stack Configuration (IP address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
0x6	Hostname	Set/Get	STRING	Hostname (for DHCP DNS Update)
0x7	Safety Network Number			Unsupported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default 1)
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)

Table 48: Attributes of Instance 1 (cont.)

Id	Attribute	Access Rule	Data type	Description
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Table 49: Hirschmann extensions to the TCP/IP Interface Object

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link object

The information in the following tables are part of the Ethernet Link Object. To access the information, use the following values:

- Class(####)
- Instance(###)
- Attribute(#)

Specify at least one instance in the device, for example, Instance 1 is the CPU Ethernet interface instance (*Class Code 0xF6*) of *EtherNet/IP*.

Table 50: Instance attributes

Id	Attribute	Access Rule	Data type	Description
0x1	Interface Speed	Get	UDINT	Used interface speed in Mbit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-negotiation Status 3: 4: 0x0=Auto-negotiation in progress 0x1=Auto-negotiation failed 0x2=Failed but speed detected 0x3=Auto-negotiation success 0x4=No Auto-negotiation 5: Manual configuration require reset (constantly 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Detected errors: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

Table 50: Instance attributes (cont.)

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in Mbit/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID

Table 51: Hirschmann extensions to the Ethernet Link Object

Id	Attribute	Access Rule	Data type	Description
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.

Table 51: Hirschmann extensions to the Ethernet Link Object (cont.)

Id	Attribute	Access Rule	Data type	Description
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 8: 9: 00001_B: Link Flap 10: 00010_B: CRC/Fragments 11: 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12: Reserved (constantly 0)
				13: Reserved (constantly 0)
				14: Reserved (constantly 0)
				15: Reserved (constantly 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables auto-negotiation, and Spanning Tree on the interface.

Table 51: Hirschmann extensions to the Ethernet Link Object (cont.)

Id	Attribute	Access Rule	Data type	Description
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Table 52: Assignment of ports to Ethernet Link Object Instances

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

Note:
The number of ports depends on the type of hardware used. The Ethernet Link Object only exists, if the port is connected.

Switch Agent object

The device supports the Hirschmann specific Ethernet Switch Agent Object (*Class Code 0x95*) for the device settings and information parameters with Instance 1.

Table 53: Class attributes

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4-5:	Reserved
				6:	Reserved
				7:	Reserved
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	ACA22-USB-C (EEC) removed (1=removed)
				12:	ACA31 removed (1=removed)
				13-22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29-30	Reserved
				31:	Connection Error (1=failure)
0x2	Switch Temperature	Get	STRUCT of:		
			INT TemperatureF	in °F	
			INT TemperatureC	in °C	
0x3	Reserved	Get	UDINT	Reserved for future use (constantly 0)	
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports	

Table 53: Class attributes (cont.)

Id	Attribute	Access Rule	Data type	Description
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

Table 53: Class attributes (cont.)

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

The Hirschmann specific Ethernet Switch Agent Object provides you with the additional vendor specific service, with the *Service Code 0x35* for saving the device settings. When you send a request from your PC to save the device settings, the device sends a reply after saving the settings in the flash memory.

Base Switch object

The Base Switch object provides the CIP application-level interface to basic status information for a managed Ethernet switch (revision 1).

Only Instance 1 of the Base Switch (*Class Code 0x51*) is available.

Table 54: Instance attributes

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Table 54: Instance attributes (cont.)

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default 300) 0=Learning off
0xC	Temperature C	Get	DINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	DINT	Switch temperature in degrees Fahrenheit

Message Router

The Message Router object *(Class Code 0x20)* distributes *Explicit Request* messages to the appropriate handler object.

Table 55: Class attributes

Id	Attribute	Access Rule	Data type	Description
1	Revision	Get	UINT	Revision: 1
2	Largest Instance Number	Get	UINT	Largest instance number: 1
3	Number of Instances Currently Existing	Get	UINT	Number of instances currently existing: 1
4	Optional Attribute List	Get	ARRAY of: BYTES	Optional attribute list: 0 Unsupported for Get_single service
5	Optional Service List	Get	ARRAY of: BYTES	Optional Service List: 0 Unsupported for Get_single service
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 0

Assembly

The Assembly object *(Class Code 0x04)* binds attributes of multiple objects. This property lets the device send or receive data to or from any object over a single connection. You can use Assembly objects to bind *Input* or *Output* data. The terms *Input* and *Output* are specified from the viewpoint of the network. *Input* produces data on the network and *Output* consumes data from the network.

Table 56: Supported instances

Instance	Description	Service
1	POWER_LINK_ASSEMBLY	Get_single
100	INPUT_ASSEMBLY_NUM	Get_single
150	OUTPUT_ASSEMBLY	Get_single/Set_single
151	CONFIG_ASSEMBLY_NUM	Get_single/Set_single

Table 56: Supported instances (cont.)

Instance	Description	Service
152	HEARBEAT_INPUT_ONLY_ASSEMBLY	Get_single/Set_single
153	HEARBEAT_LISTEN_ONLY_ASSEMBLY	Get_single/Set_single
154	EXPLICT_ASSEMBLY	Get_single/Set_single

Table 57: Class attributes

Id	Attribute	Access rule	Data type	Description
1	Revision	Get	UINT	Revision: 2
2	Largest Instance Number	Get	UINT	Largest instance number: 154
3	Number of Instances Currently Existing	Get	UINT	Number of instances currently existing: 7
4	Optional Attribute List			Unsupported
5	Optional Service List			Unsupported
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 4

Table 58: Instance attributes

Id	Attribute	Access Rule	Data type	Description
3	Data	Get	ARRAY of: BYTES	
4	Size	Get	UINT	Number of bytes in Attribute 3

Connection Manager

The Connection Manager Class (*Class Code 0x06*) allocates and manages the internal resources associated with both *I/O* and *Explicit Messaging* connections.

Table 59: Class attributes

Id	Attribute	Access rule	Data type	Description
1	Revision	Get	UINT	Revision: 1
2	Largest Instance Number	Get	UINT	largest instance number: 1
3	Number of Instances Currently Existing	Get	UINT	Number of instances currently existing: 1
4	Optional Attribute List			Unsupported

Table 59: Class attributes (cont.)

Id	Attribute	Access rule	Data type	Description
5	Optional Service List			Unsupported
6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 14

QoS object

The QoS object (0x48) provides sending EtherNet/IP messages with non-zero DiffServ code points (DSCP). The QoS object supports one instance.

Table 60: Class attributes

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 1
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently added: 1
0x4	Optional Attribute List			Unsupported
0x5	Optional Service List			Unsupported
0x6	Maximum ID Number Class Attributes	Get	UINT	Maximum ID Number Class Attributes: 7
0x7	Maximum ID Number Instance Attributes	Get	UINT	Maximum ID Number Instance Attributes: 8

Table 61: Instance attributes

Id	Attribute	Access Rule	Data type	Description
0x1	802.1Q TagEnable			Unsupported
0x2	DSCP PTP Event			Unsupported
0x3	DSCP PTPGeneral			Unsupported
0x4	DSCP Urgent	Get/Set	USINT	DSCP value for CIP transport class 0/1 Urgent priority messages. (default 55)
0x5	DSCP Scheduled	Get/Set	USINT	DSCP value for CIP transport class 0/1 Scheduled priority messages. (default 47)

Table 61: Instance attributes (cont.)

Id	Attribute	Access Rule	Data type	Description
0x6	DSCP High	Get/Set	USINT	DSCP value for CIP transport class 0/1 High priority messages. (default 43)
0x7	DSCP Low	Get/Set	USINT	DSCP value for CIP transport class 0/1 Low priority messages. (default 31)
0x8	DSCP Explicit	Get/Set	USINT	DSCP value for CIP explicit messages (transport class 2/3 and UCMM) and all other EtherNet/IP encapsulation messages. (default 27)

Services, Connections and I/O Data

The device supports the following connection types and parameters.

Table 62: Settings for integrating a new module

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Table 63: Device I/O data structure

I/O Data	Value (data types and sizes to be defined)	Direction	Size [1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm [2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm [3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

Table 63: Device I/O data structure (cont.)

I/O Data	Value (data types and sizes to be defined)	Direction	Size [1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. The default size of the port bit masks is 32 bits (DWORD). For devices with more than 28 ports the port bit masks have been extended to n * DWORD.
2. You specify the utilization alarm settings in the *Basic Settings > Port* dialog, *Ingress Utilization* tab. The upper threshold value is the limit, where the alarm condition becomes active. The lower threshold value is the limit, where an active alarm condition becomes inactive.
3. You specify the Access Violation alarm settings in the *Network Security > Port Security* dialog. The upper threshold value is the limit, where the alarm condition becomes active. The lower threshold value is the limit, where an active alarm condition becomes inactive.

Table 64: Mapping of the data types to bit sizes

Object type	Bit size
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

16.4 PROFINET function

PROFINET is an industrial communication protocol that is deployed worldwide. It is based on the protocols *TCP/IP* and *UDP/IP* over Ethernet. This is a crucial aspect in fulfilling the requirements for consistency from the management level right down to the field level.

PROFINET enhances the existing Profibus technology for applications that require fast data communication and the use of industrial IT functions.

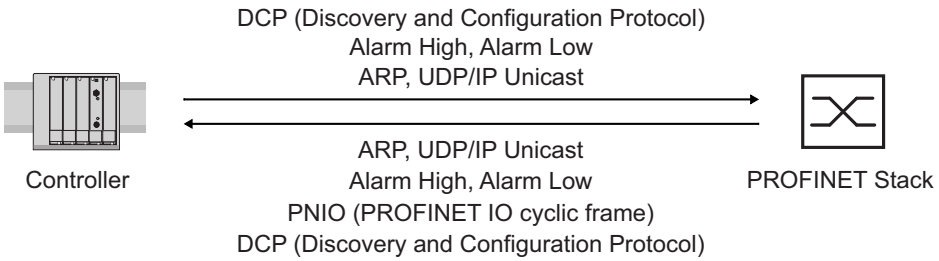


Figure 51: Communication between the Controller and the device

In particular, you find *PROFINET* in Europe and with Siemens controllers.

PROFINET uses the device description language GSDML (Generic Station Description Markup Language, based on XML) to describe devices and their properties so that they can be processed automatically. You find the device description in the GSD (Generic Station Description) file of the device.

For further information on PROFINET, see the PROFIBUS Organization website at www.profibus.com.

The devices conform to class B for *PROFINET*.

16.4.1 Device Models for PROFINET GSDML Version 2.41

The device generates GSDML files in the GSDML V.2.41 format. Within the GSDML file, the device is modeled according to GSDML standard V.2.4.

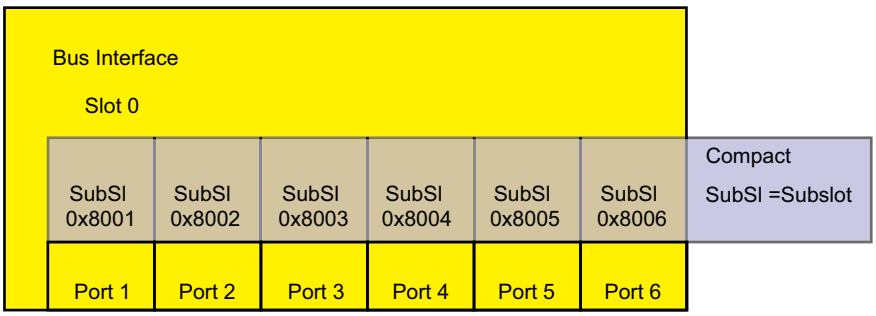


Figure 52: Compact device

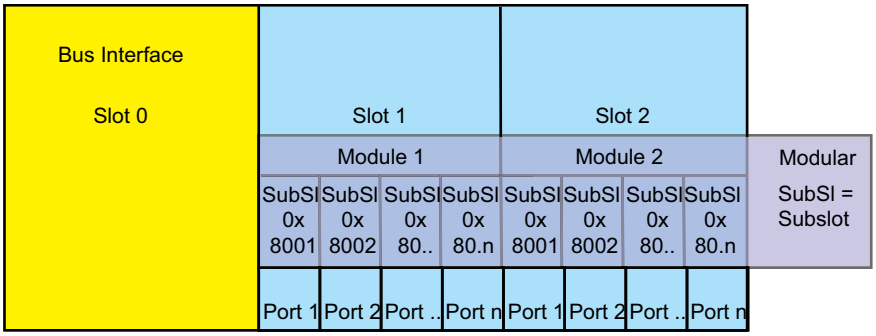


Figure 53: Modular device

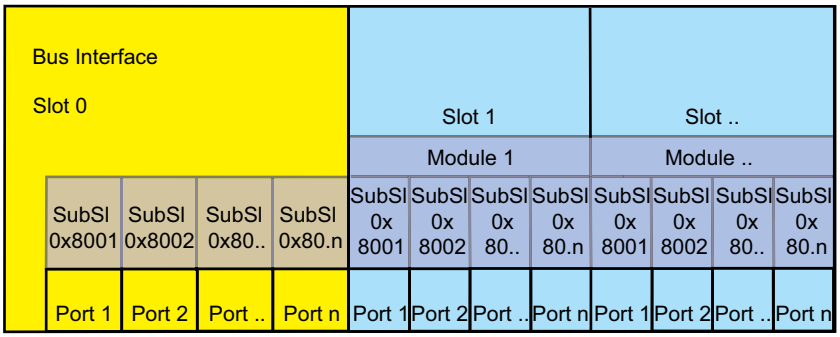


Figure 54: Mixed device

16.4.2 Graphical User Interface and Command Line Interface

When you set up the device successfully in a *PROFINET* environment, the PROFINET IO controller establishes an Application Relation (AR) with the device.

After the user logs into the device management through the Command Line Interface, the device displays a message that an Application Relation is active. In the *Advanced > Industrial Protocols >* PROFINET dialog, the Graphical User Interface displays equivalent information, for example, the number of running Application Relations.

16.4.3 Integrating the device into a Control System

Preparing the device

First you install, connect and set up the device. Then you integrate the device into a Control System. To do this, perform the following steps:

- ☐ Open the *Basic Settings > System* dialog.
- ☐ Verify that a valid system name for the device is specified in the *System name* field.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Basic Settings > Network > IPv4* dialog.
- ☐ In the *Management interface* frame, select the *Local* radio button.

- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Switching > VLAN > Configuration* dialog.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Diagnostics > Status Configuration > Device Status* dialog, *Global* and *Port* tabs.
- ☐ Set up the alarms you want to monitor.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.
- ☐ Open the *Advanced > Industrial Protocols > PROFINET* dialog.
- ☐ Download the GSD(ML) file and the icon onto your local computer.
- ☐ Enable the *PROFINET* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Apply the settings temporarily. To do this, click the ✓ button.

Changing the default values

Functions that directly affect the *PROFINET* function require the following default values to be changed. When you obtain the device as a specially available *PROFINET* variant, the following values are already predefined:

PROFINET	*Advanced > Industrial Protocols > PROFINET* dialog • *Operation* = *On* • *Name of station* = "" (empty string)
Network	*Basic Settings > Network > Global* dialog • *HiDiscovery protocol v1/v2 Access* = *readOnly* *Basic Settings > Network > IPv4* dialog • *IP address assignment* = *Local* • *IP address* = 0.0.0.0 • *Netmask* = 0.0.0.0 • *Gateway address* = 0.0.0.0
VLAN ID	*Switching > VLAN > Configuration* dialog • *VLAN ID* = 1 The uplink port is a member of VLAN 1 and transmits the data packets with a VLAN tag.
LLDP	*Diagnostics > LLDP > Configuration* dialog • *Transmit interval [s]* = 5 • *Transmit delay [s]* = 1

Configuring the PLC

The following illustrates the configuration of the PLC using the example of the TIA Portal software from Siemens, and assumes that you are familiar with operating the software.

The device also supports engineering stations from other manufacturers, such as PC Worx from Phoenix Contact.

In the PLC default setting, the PLC detects the interruption of the I/O connection to the device and treats the interruption as a failure. The PLC considers 3 consecutive real time packets missing from a partner PLC or from the device as an interruption. According to the default setting, the PLC treats this as a system failure. To change this default setting, you employ TIA Portal programming measures.

Note:
Monitoring the I/O connection to the CPU of the device as a detected failure can result in a potential system failure. Therefore, do not consider the I/O connection to the CPU when monitoring.
The device management data packets can interrupt the I/O connection between the PLC and the device. For example, a management station can saturate the CPU of the device with higher priority real time data. In this case, because the device can still transmit or receive data packets, the system remains operational.

Providing the GSDML file

The Hirschmann device provides you with the following option for generating GDSML files and icons:

- You can use the *Advanced > Industrial Protocols > PROFINET* dialog in the GUI to download the GSDML file and the icon of the device.

16.4.4 Incorporating the device in the configuration

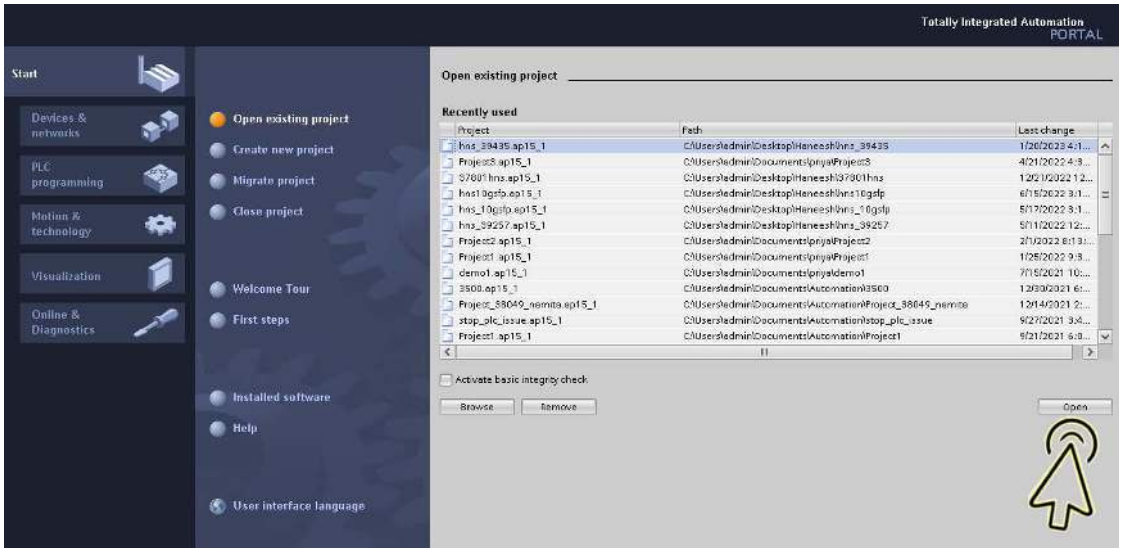
Incorporating the GSDML-based device in the network device settings includes the following actions:

- “Incorporating the device” on page 314
- “Renaming the device” on page 319
- “Setting up the IO Cycle” on page 324
- “Setting up Media Redundancy” on page 330
- “Adding modules for modular devices” on page 336
- “Adding digital I/O modules in non-modular devices” on page 340
- “Adding digital I/O modules in modular devices” on page 344
- “Adding an SFP transceiver as a submodule in non-modular devices” on page 348
- “Configuring the port properties” on page 351
- “Configuring the connection options” on page 356
- “Swapping devices” on page 365
- “Topology discovery” on page 366
- “Configuring the topology” on page 366
- “Communication diagnosis” on page 366

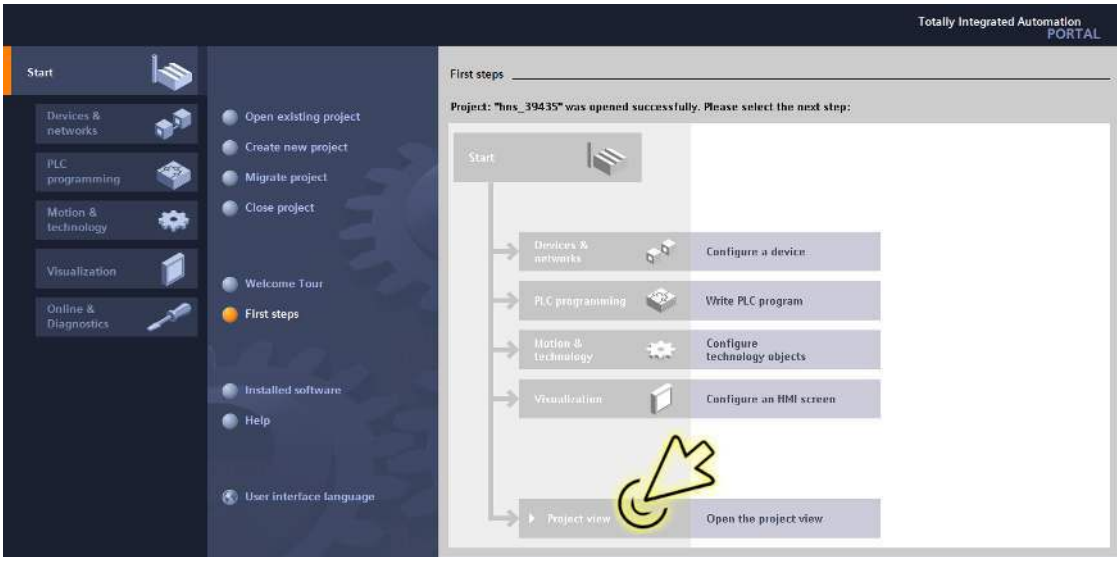
Incorporating the device

Perform the following steps:

- ☐ Open the *TIA Portal* application.
- ☐ Open your project. To do this, select your project and click the *Open* button.

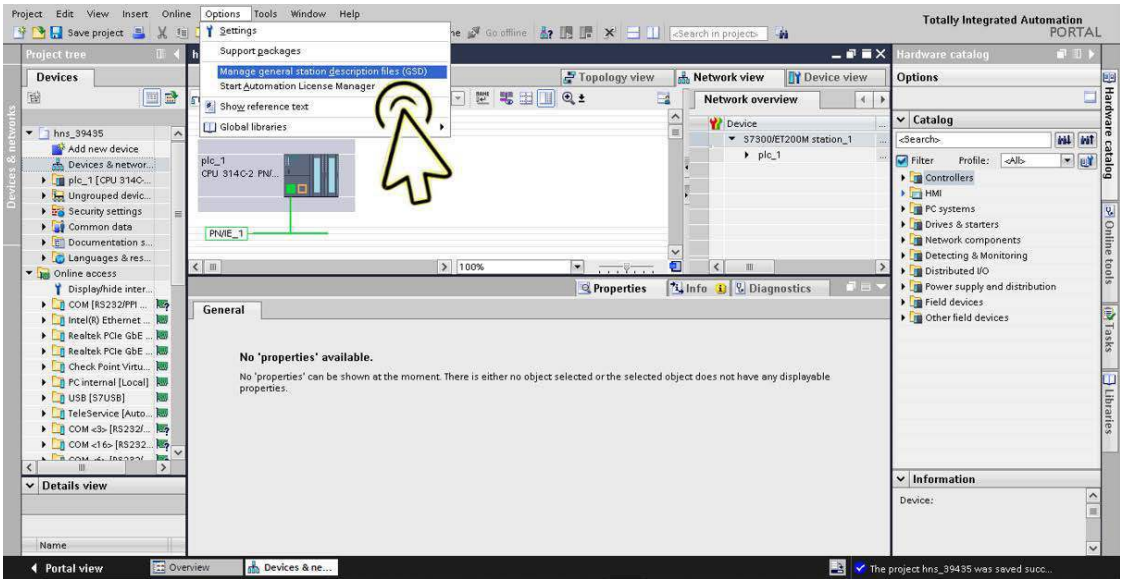


- ☐ In the *Project view* frame, select the *Open the project view* object.

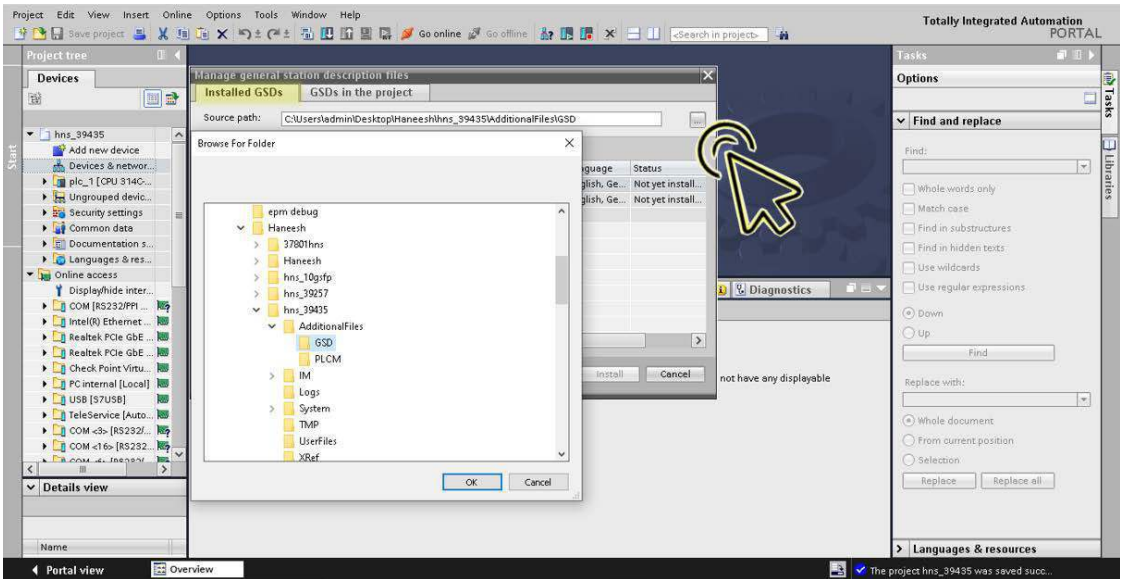


- ☐ Install the GSDML file.

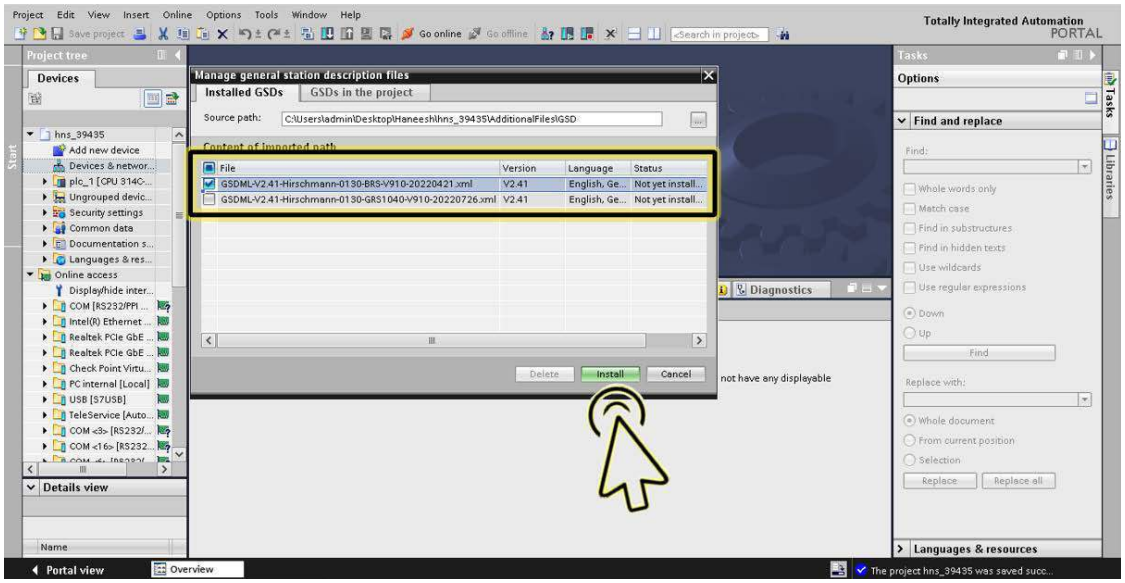
– In the menu bar, click the items *Options > Manage general station description files (GSD)*.



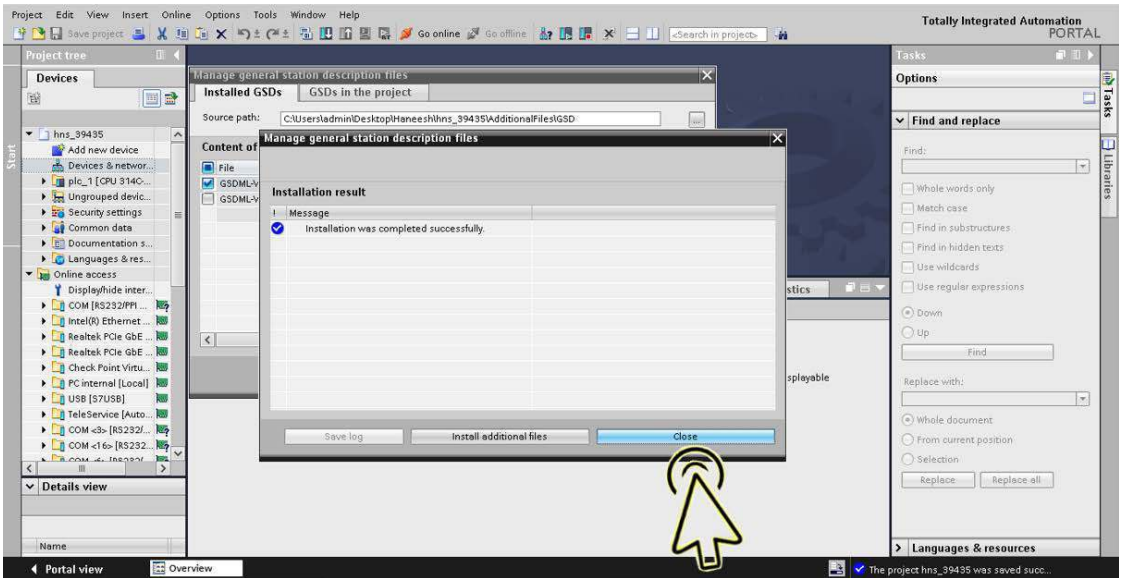
– In the *Manage general station description files* dialog, *Installed GSDs* tab, *Source path* field, browse and select the GSD folder for the GSDML file previously saved on your computer. Click the *OK* button.



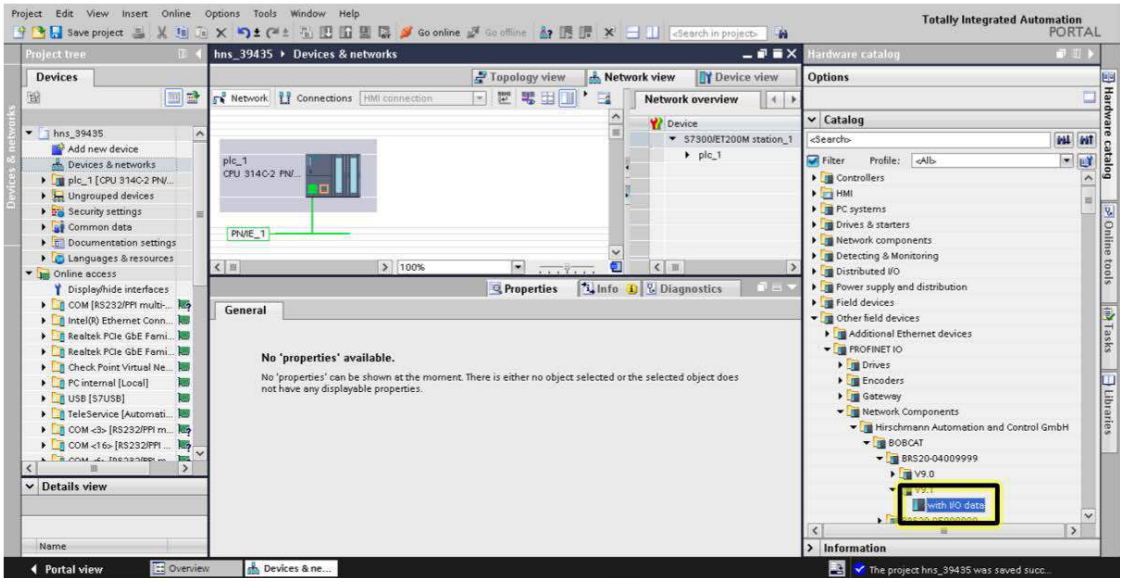
– Mark the GSDML file and click the *Install* button.



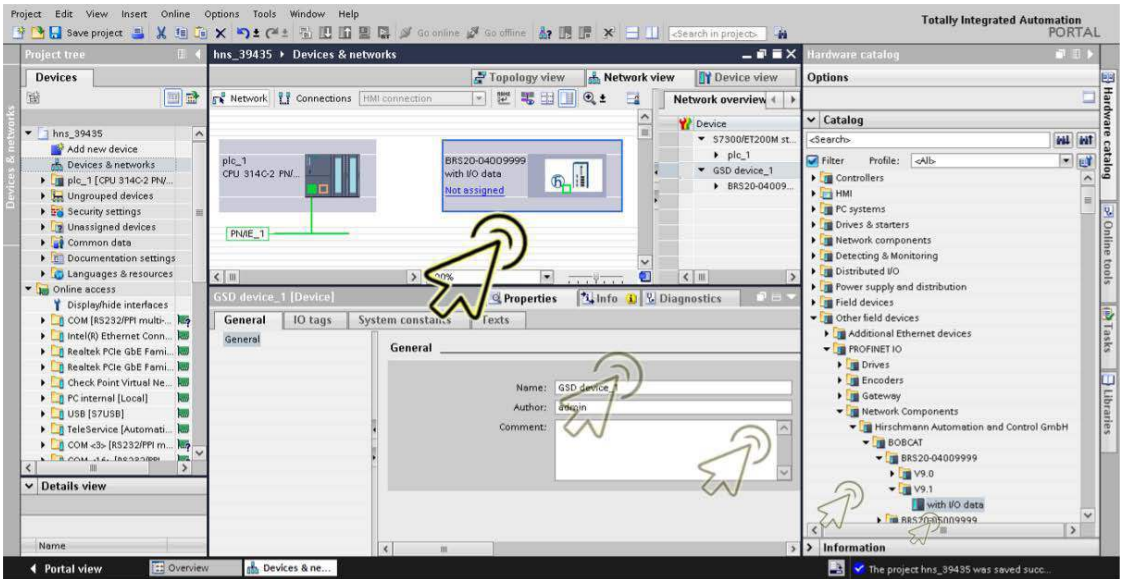
– After the GSDML file installation is completed, click the *Close* button.



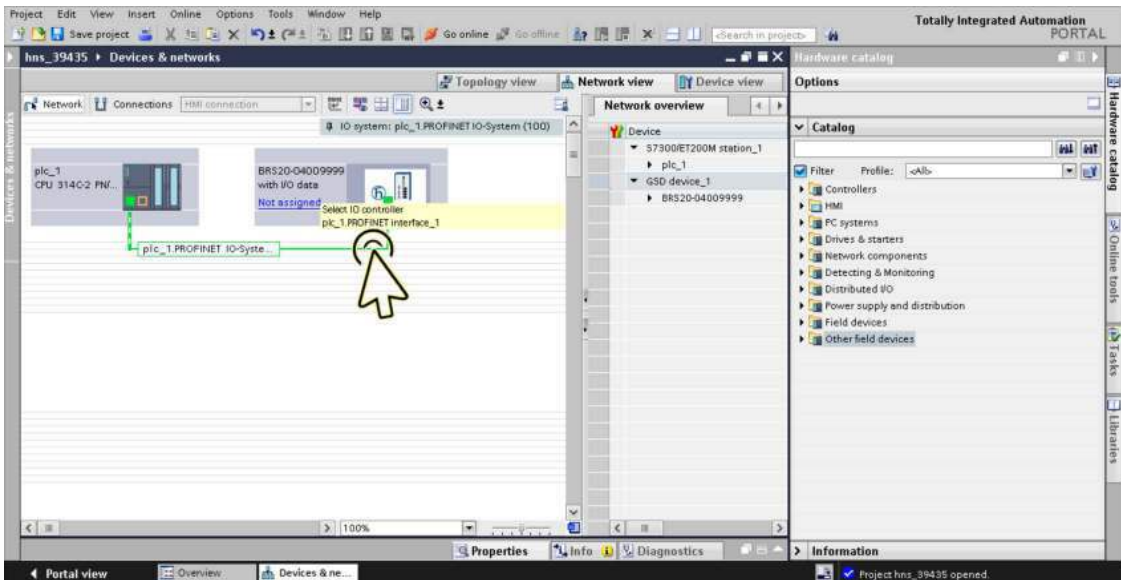
You find the new device under the items *Other field devices > PROFINET IO > Network Components > Hirschmann Automation and Control GmbH*.



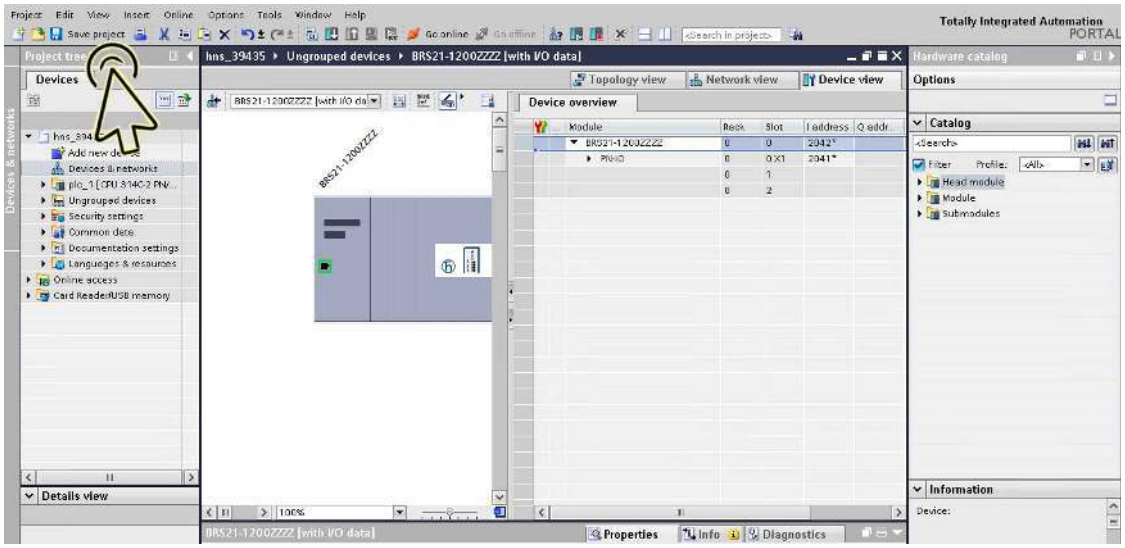
☐ Drag the selected device and drop it onto the *Network view* worksheet.



☐ Assign the device to the PLC. To do this, click the *Not assigned* link in the device tile, then select the required item.



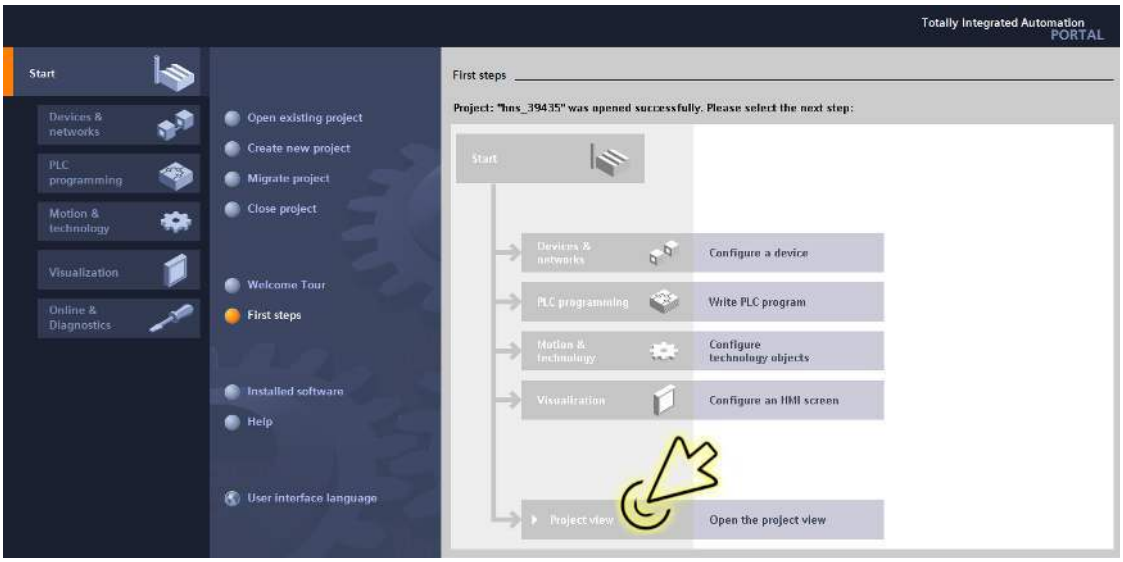
☐ Click the *Save project* icon.



Renaming the device

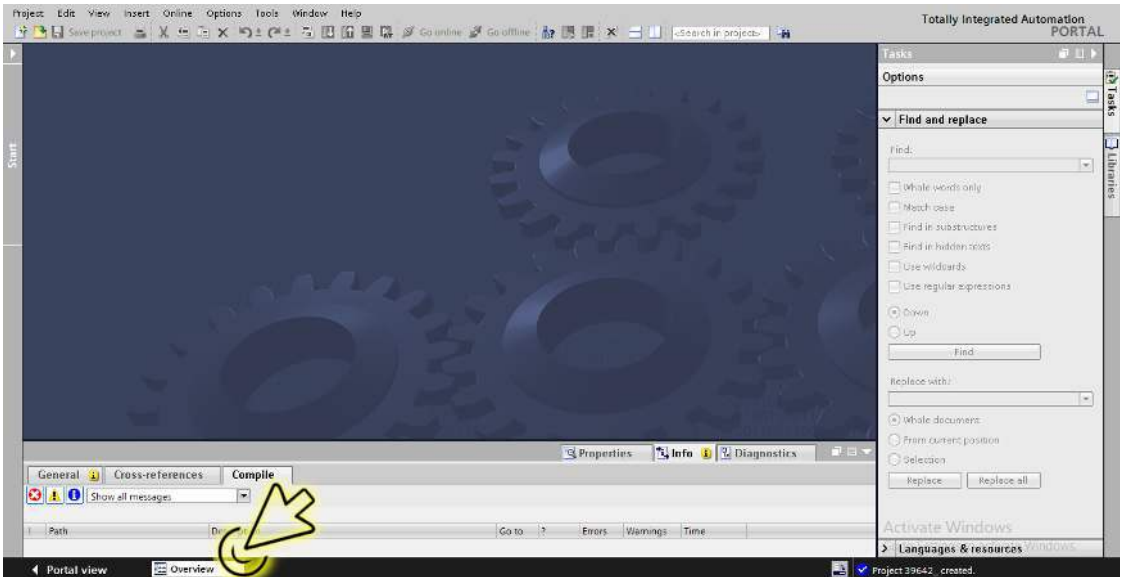
Perform the following steps:

☐ Click the *Project view* icon.



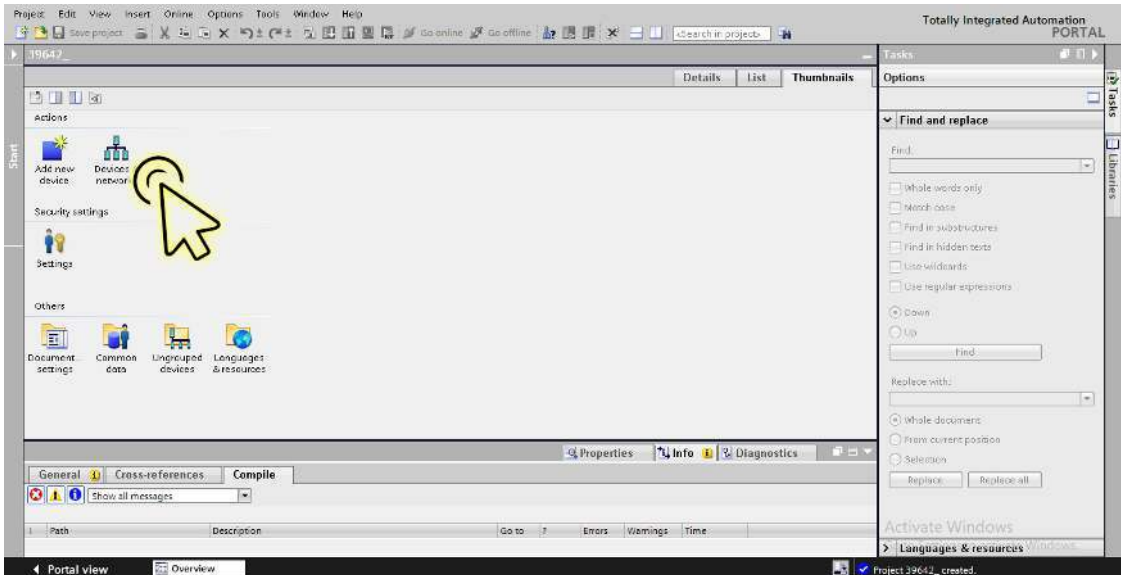
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



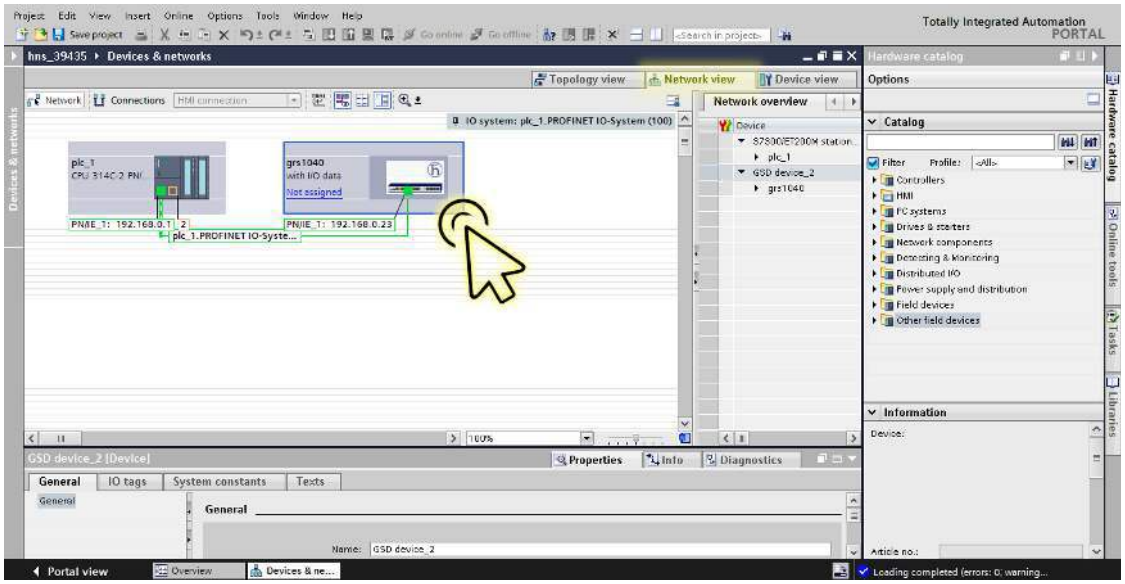
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

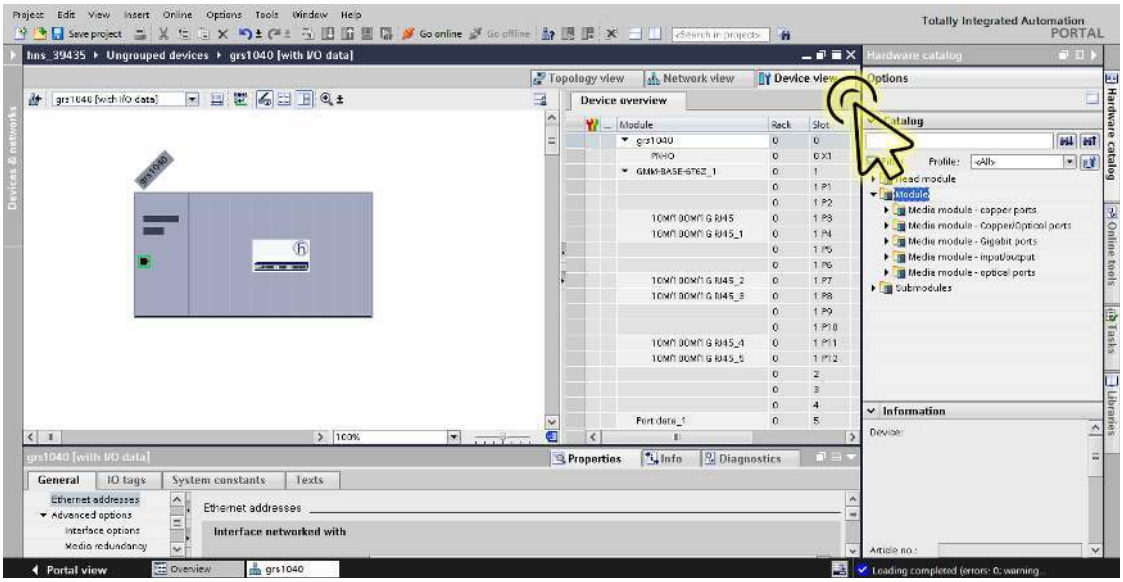


The dialog displays the *Devices & networks* window.

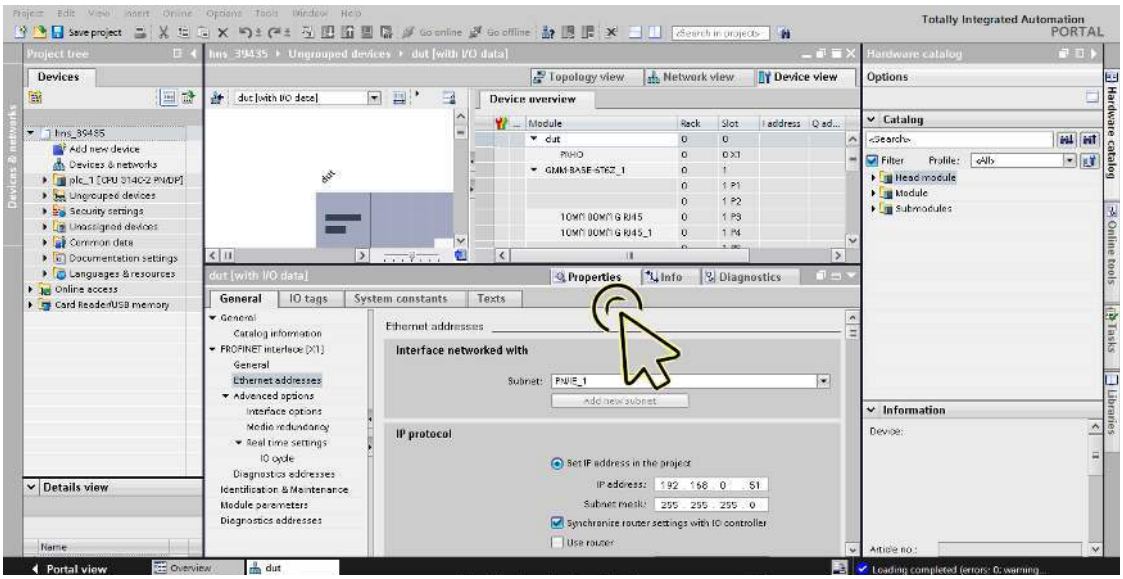
☐ In the *Network view* tab, click the icon of the device.



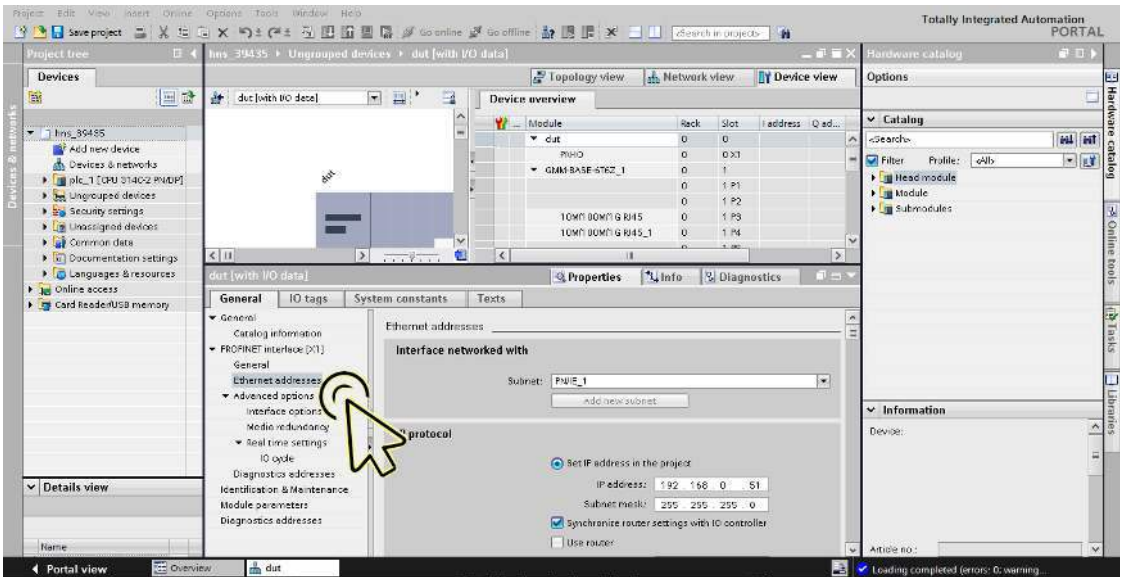
☐ Select the *Device view* tab to display the device details.



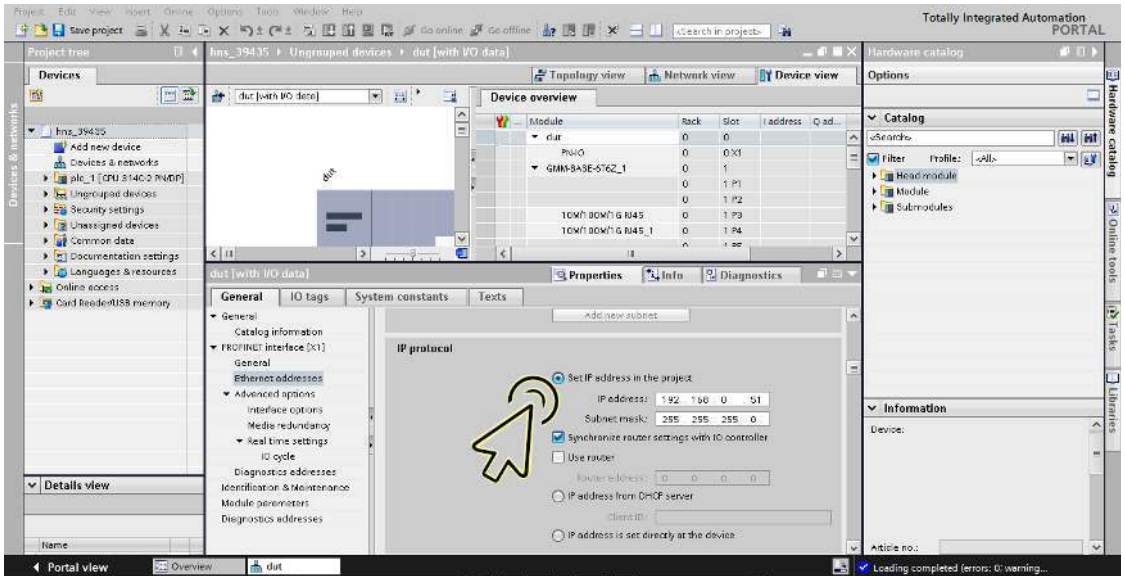
☐ Select the *Properties* tab. The *Properties* tab contains additional tabs.



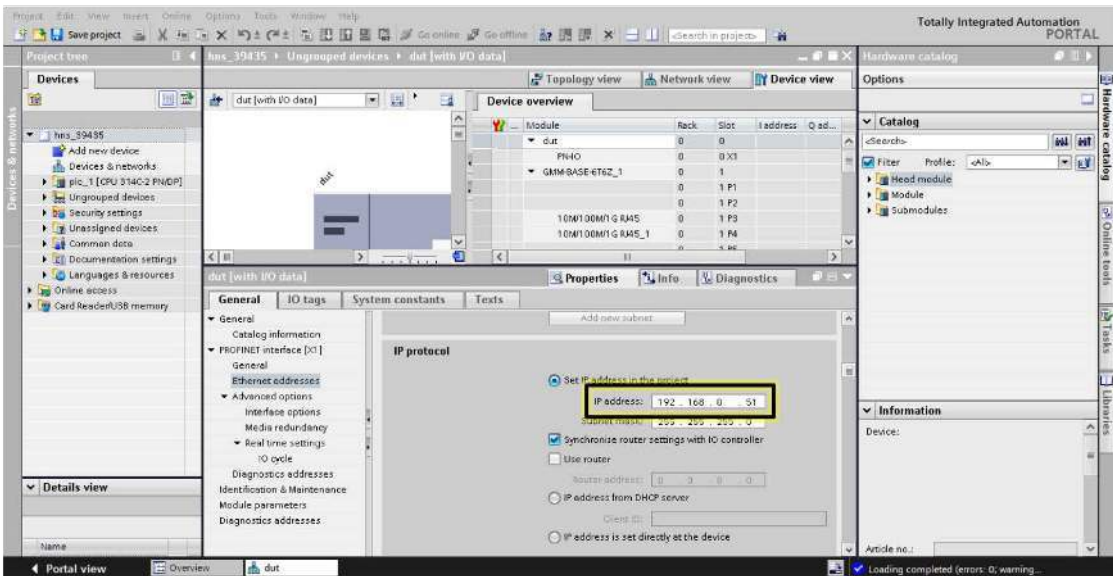
☐ In the tree view, *PROFINET interface [X1]* branch, select the *Ethernet addresses* item.



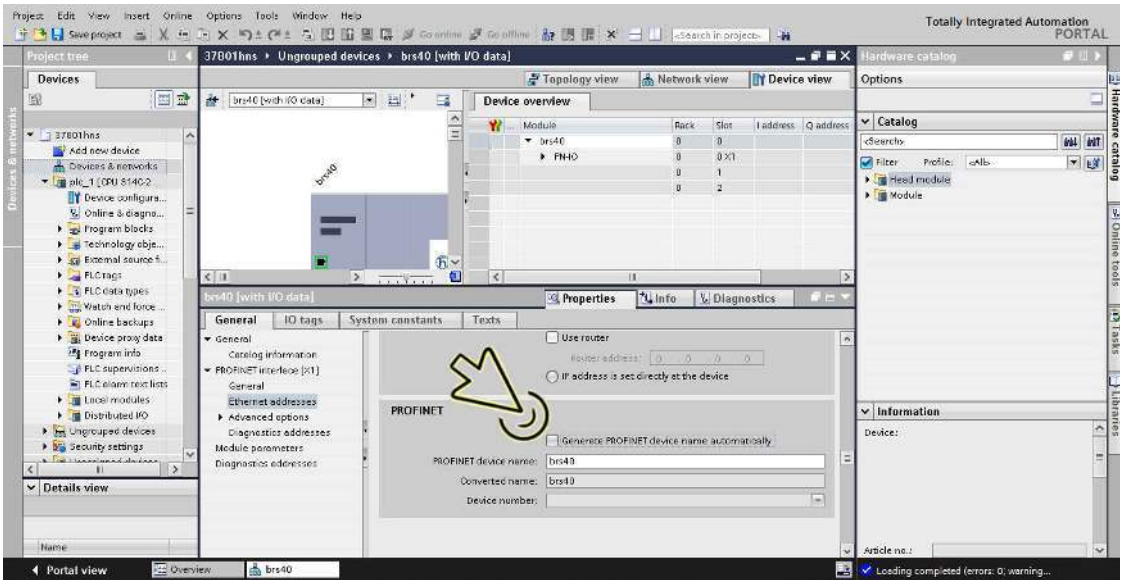
☐ In the *IP protocol* frame, select the *Set IP address in the project* radio button.



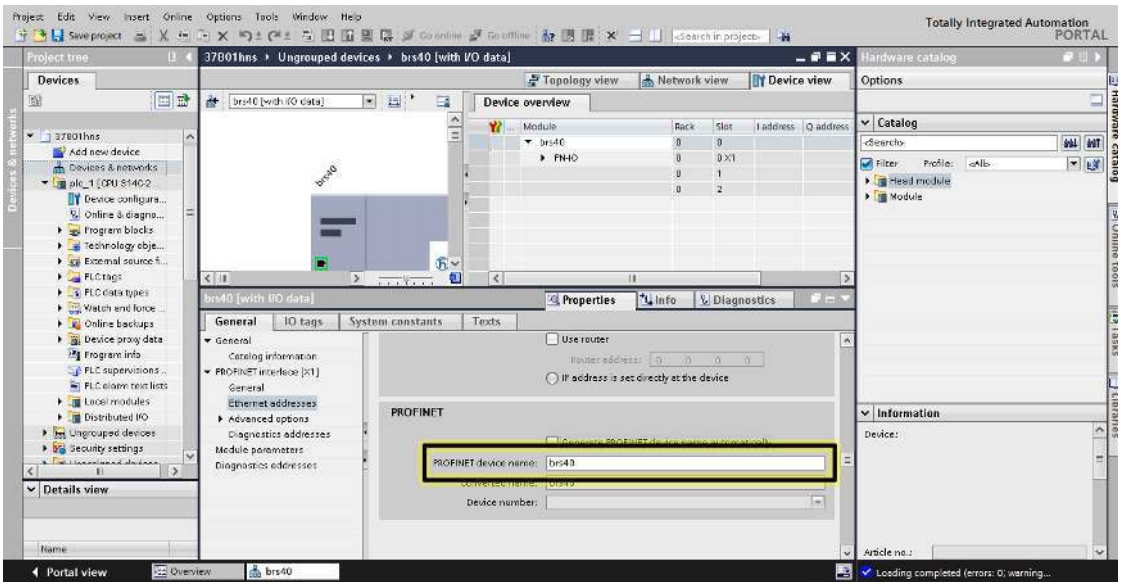
☐ In the *IP address* field, enter the required IP address.



☐ In the *PROFINET* frame, unmark the *Generate PROFINET device name automatically* checkbox.



☐ Enter the same name as specified in the Hirschmann device in the *PROFINET device name* item.

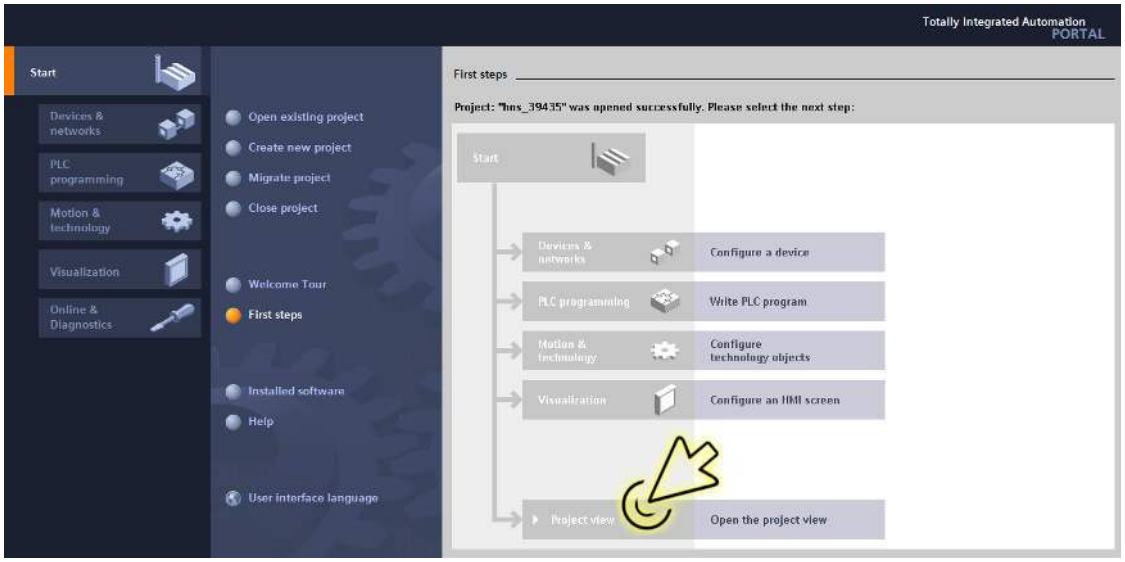


The device is now included in the configuration.

Setting up the IO Cycle

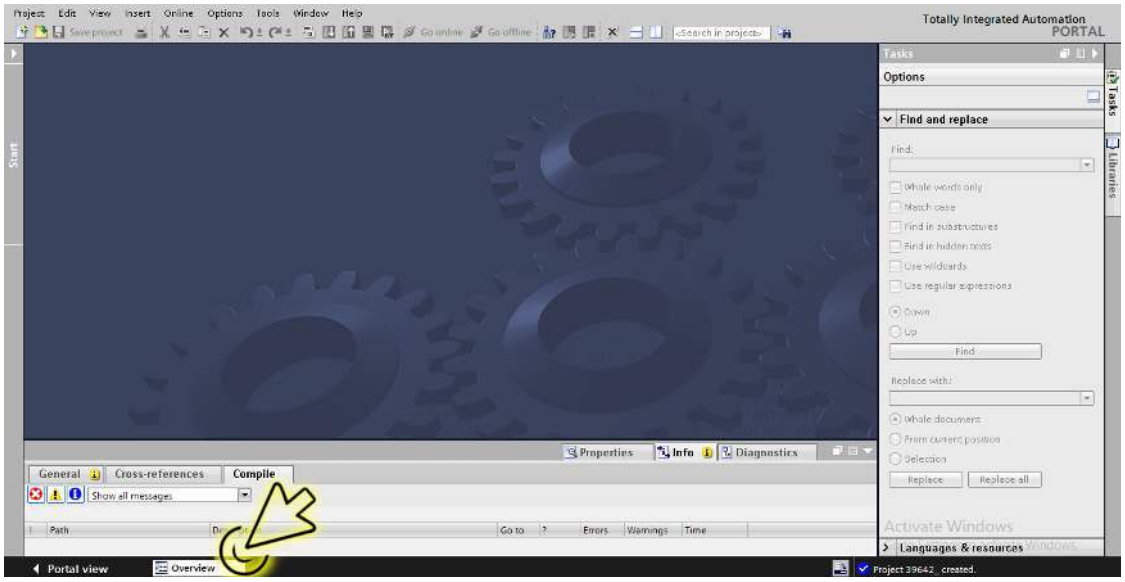
Perform the following steps:

☐ Click the *Project view* icon.



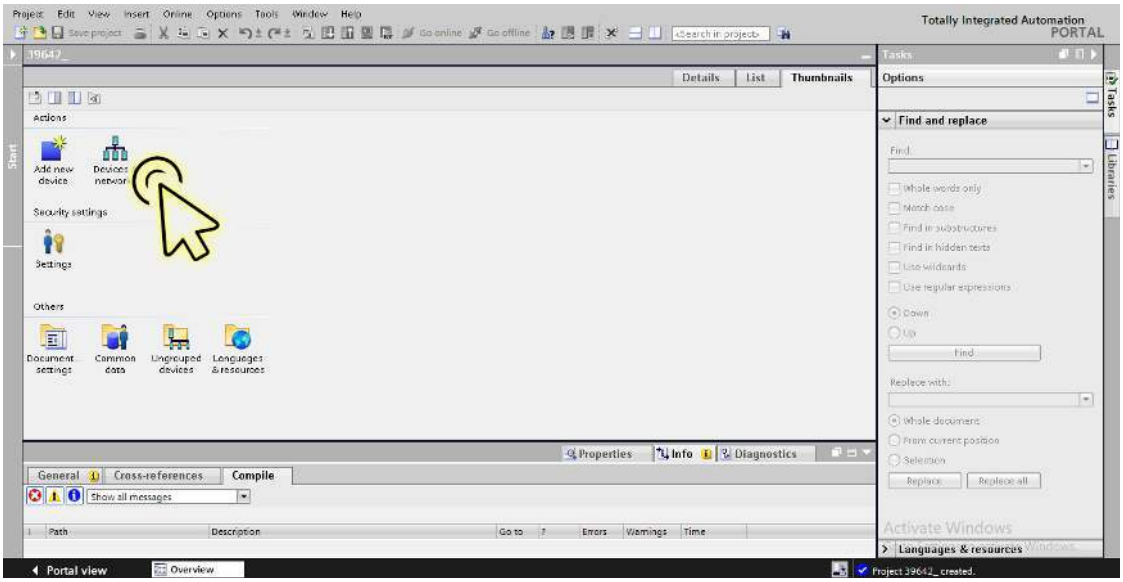
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



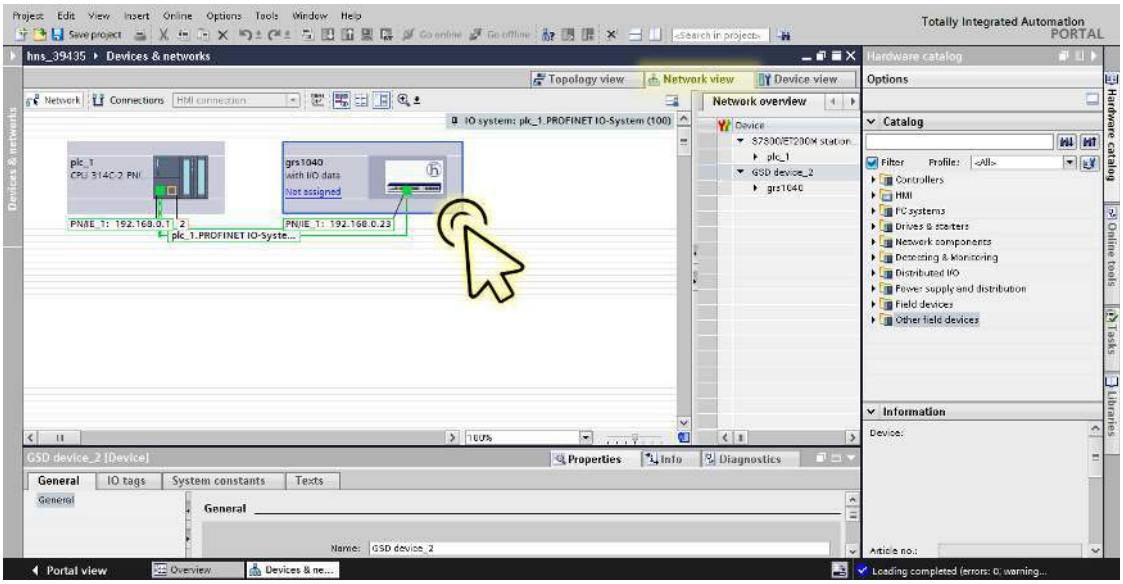
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

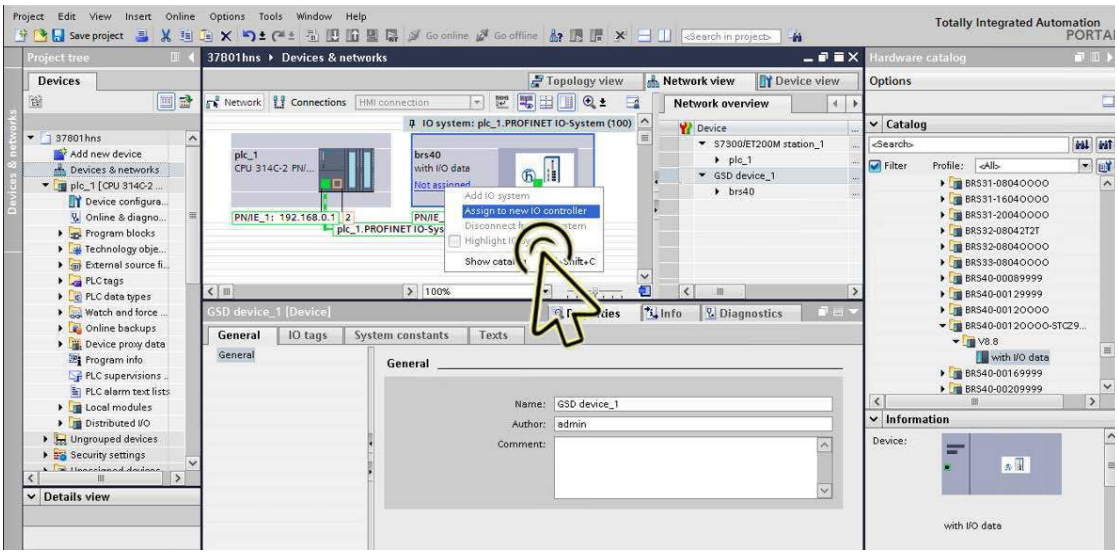


The dialog displays the *Devices & networks* window.

☐ In the *Network view* tab, click the icon of the device.

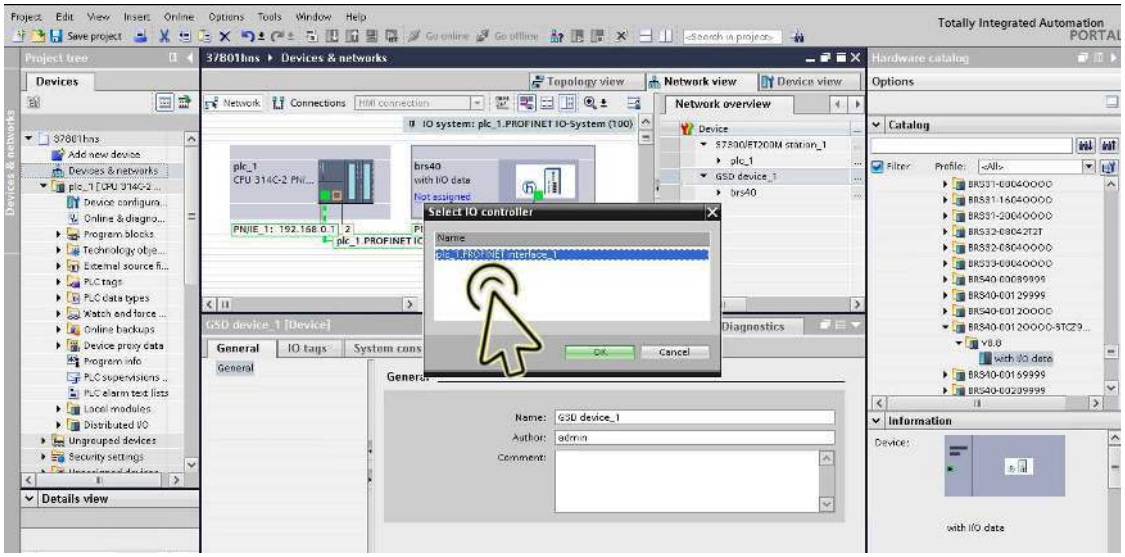


- Assign the device to the PLC.
  - Right-click the *Not assigned* link in the device tile.
  - In the context menu, select the *Assign to new IO controller* item.



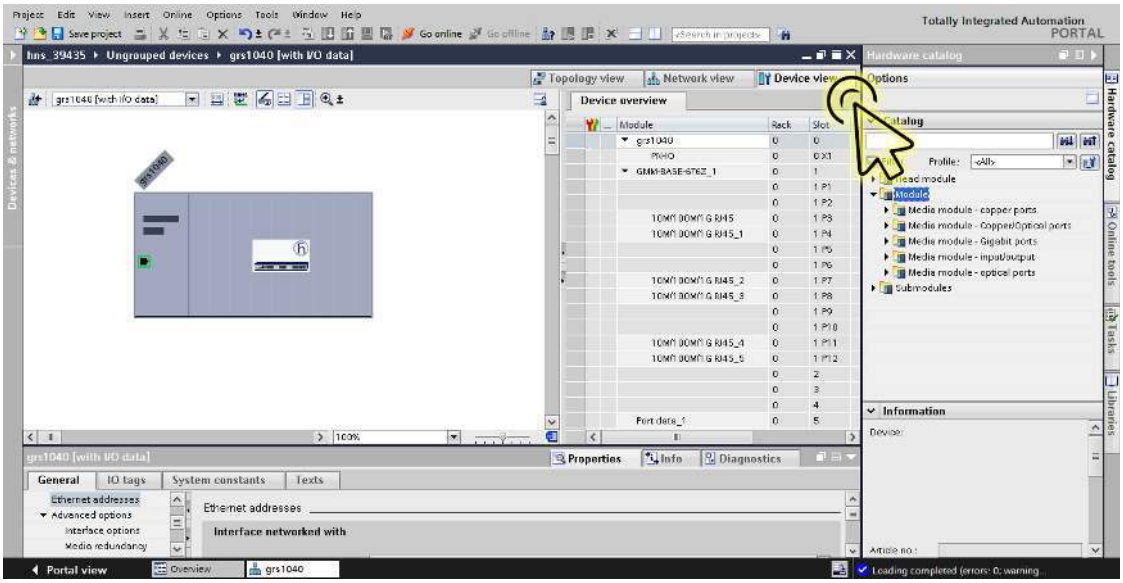
The *Select IO controller* window opens.

- Select the required item, then click the *OK* button.

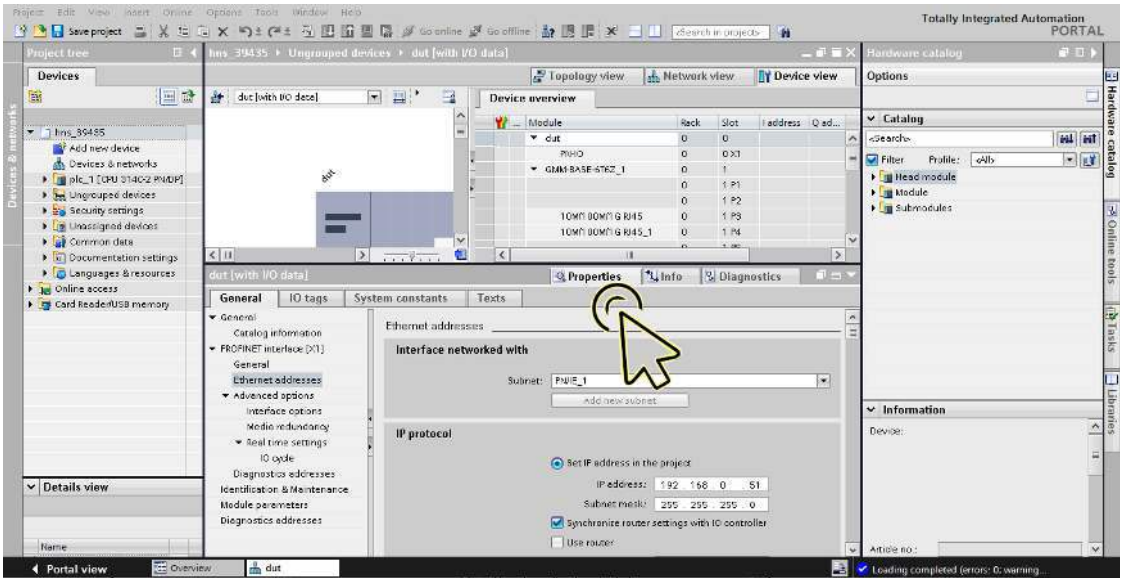


As an alternative, click the *Not assigned* link in the device tile, then select the required item.

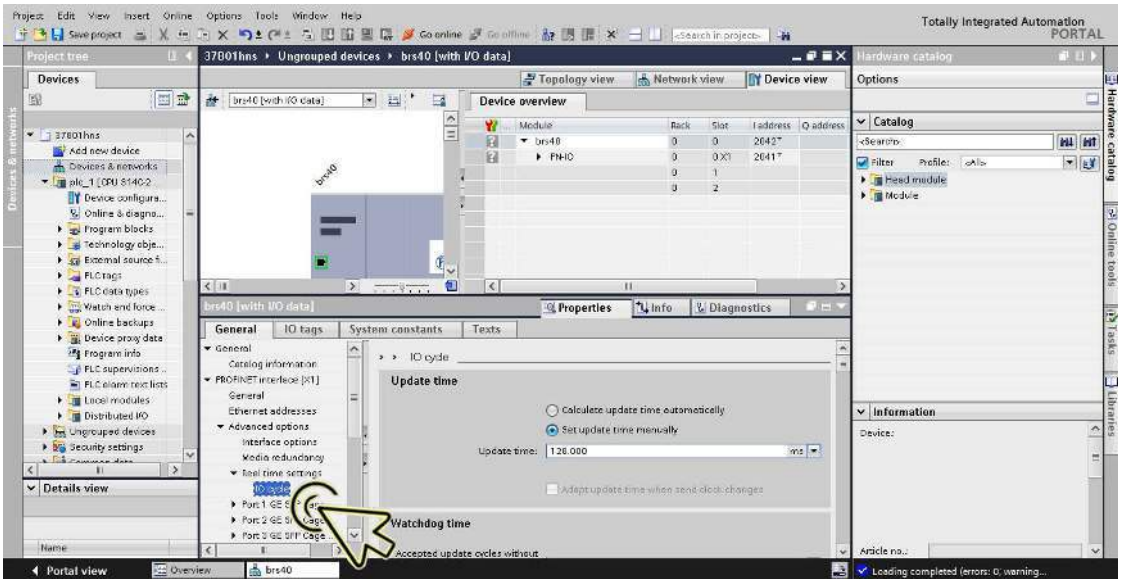
☐ Select the *Device view* tab to display the device details.



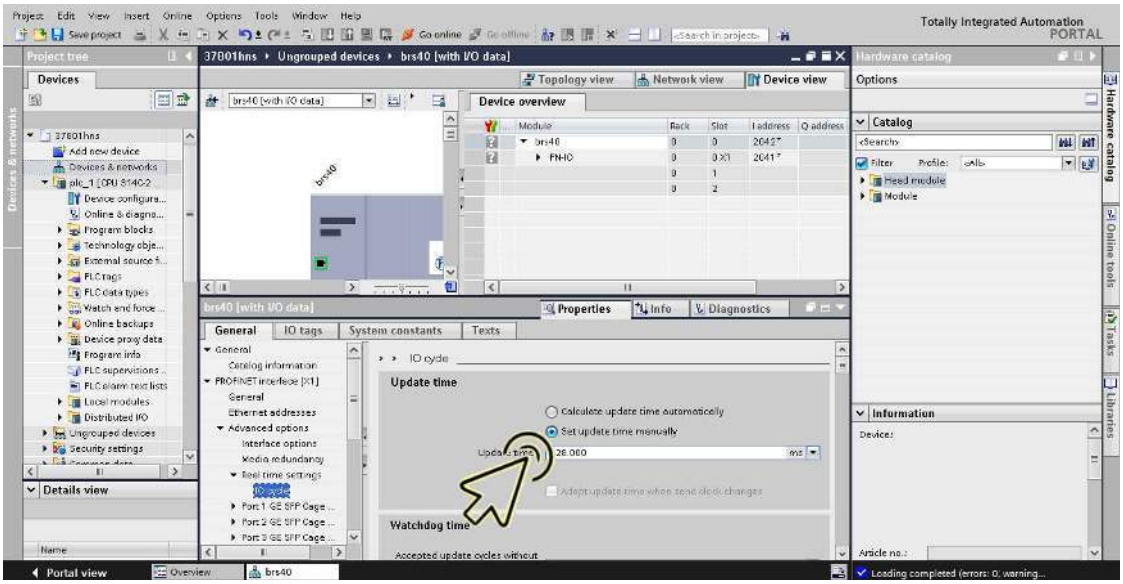
☐ Select the *Properties* tab.
The *Properties* tab contains additional tabs.



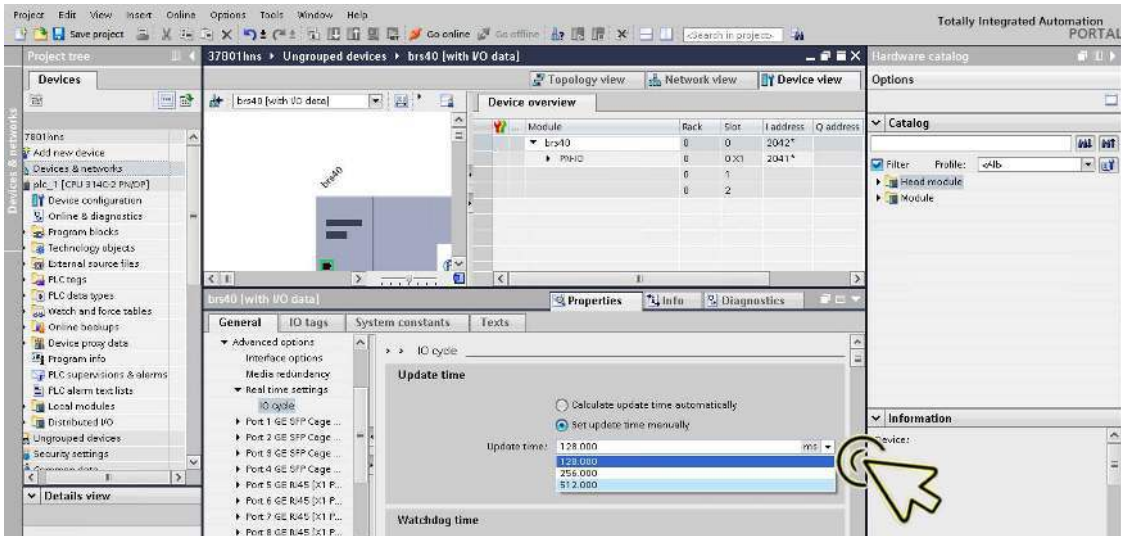
☐ In the *General* tab, navigate to the *PROFINET interface [X1] > Advanced options > Real time settings > IO cycle* item.



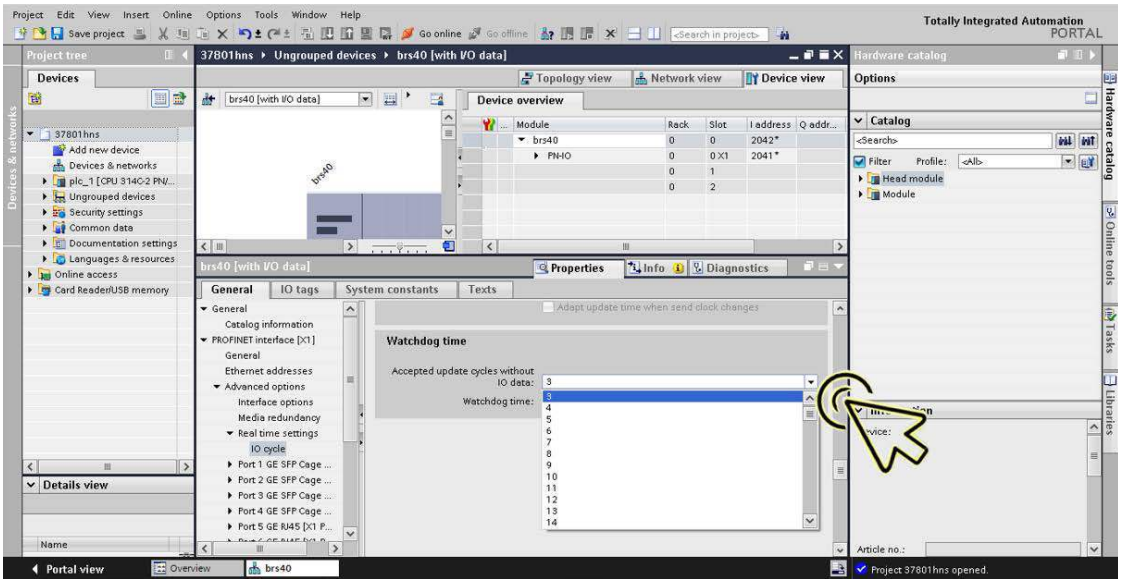
☐ In the *Update time* frame, select the *Set update time manually* radio button.



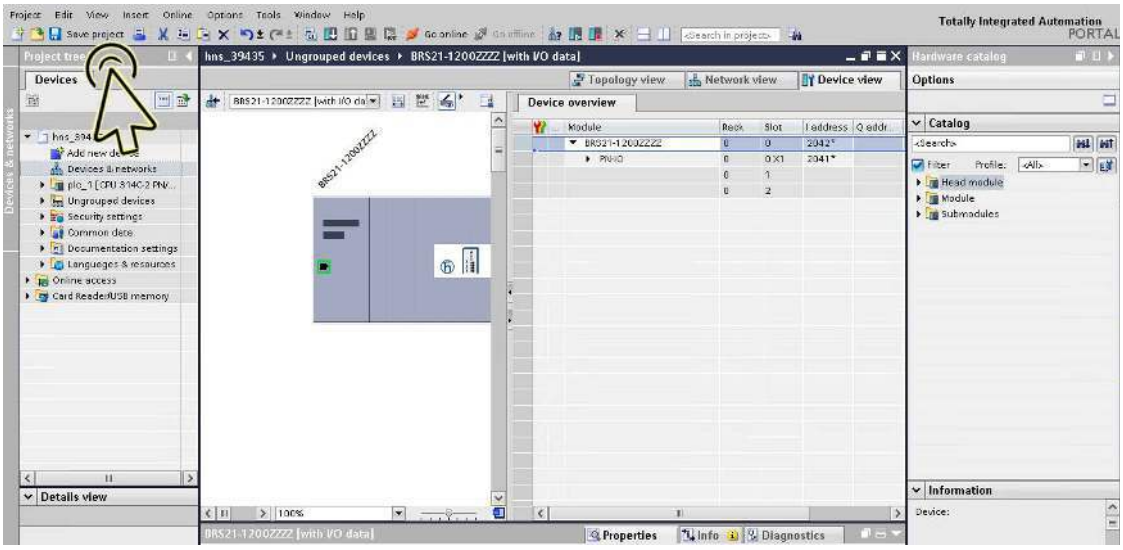
☐ From the *Update time[ms]* drop-down list, select the desired item.



- In the *Watchdog time* frame, select the desired item from the *Accepted update cycles without IO data* drop-down list.



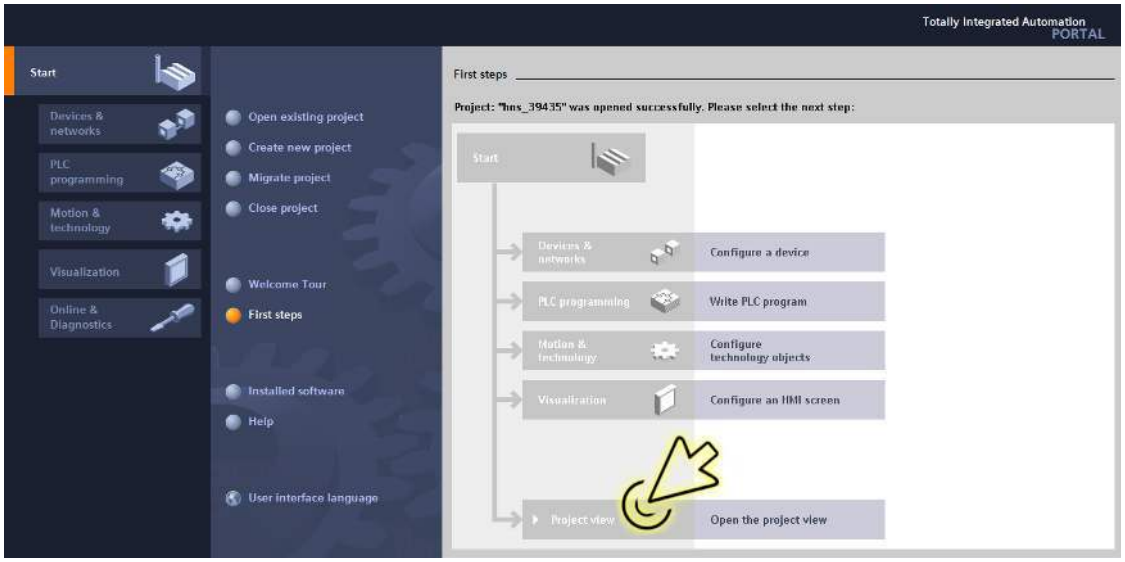
- Click the *Save project* button.



Setting up Media Redundancy

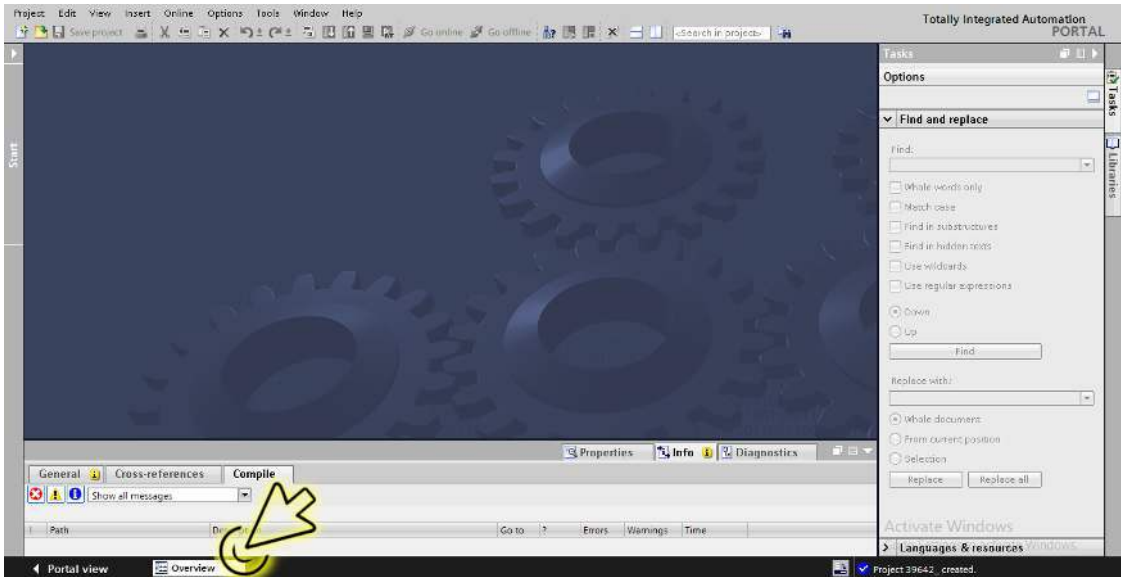
Perform the following steps:

☐ Click the *Project view* icon.



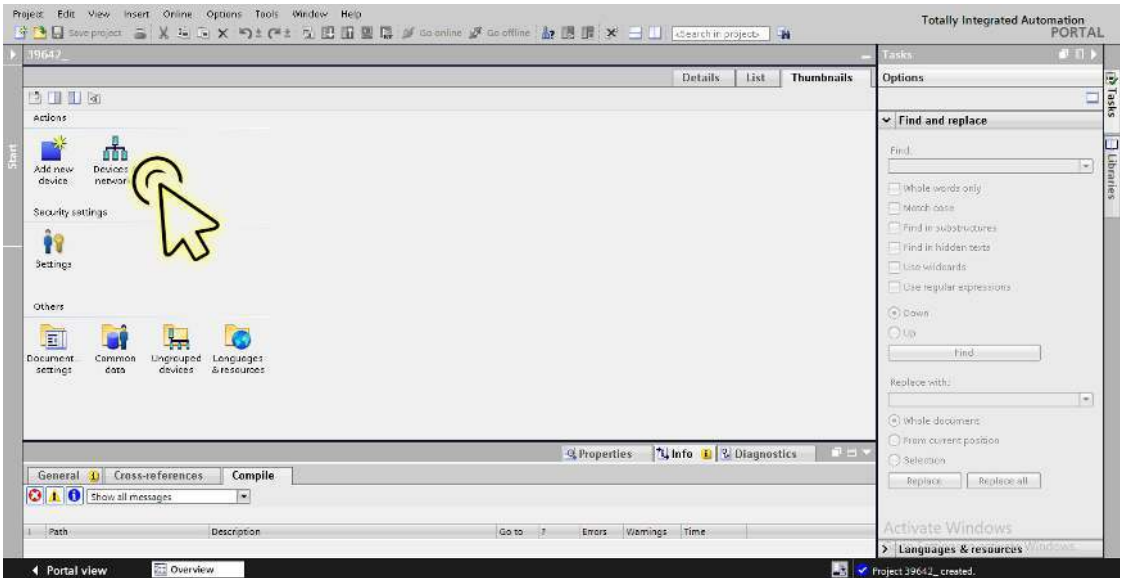
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



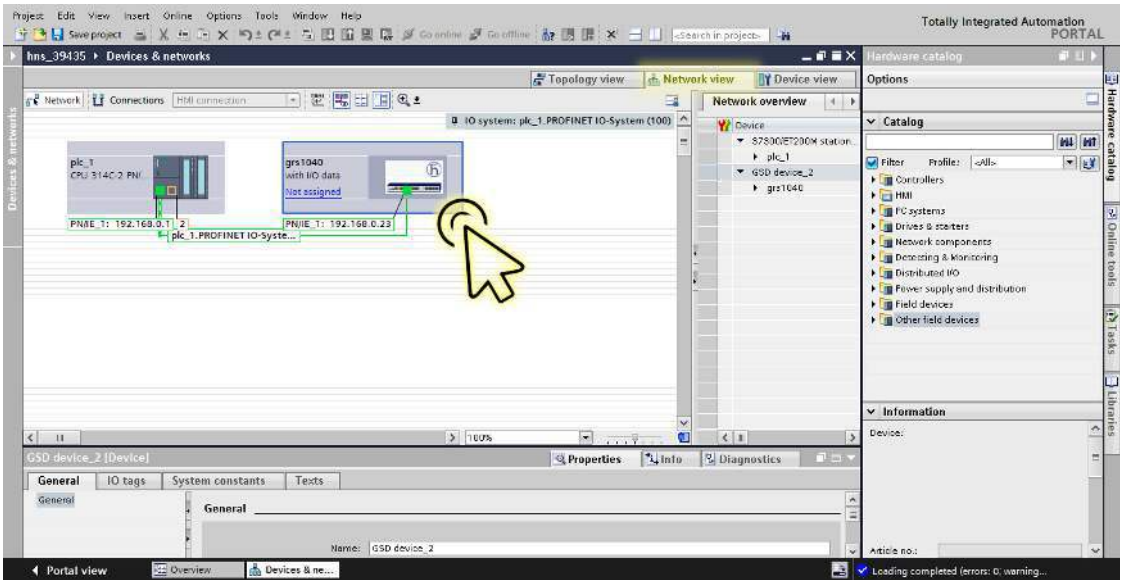
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

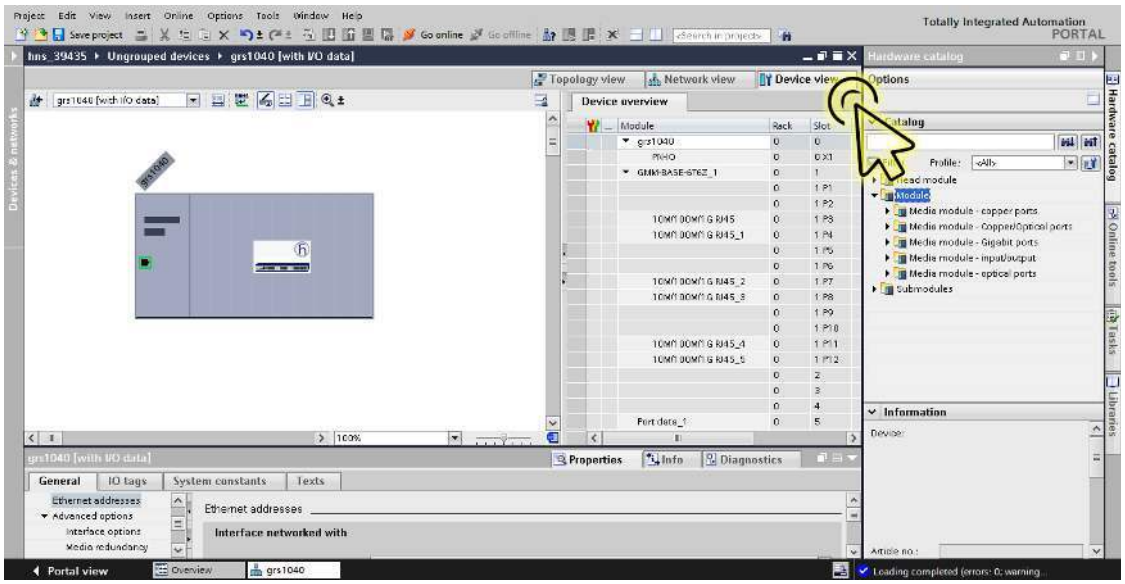


The dialog displays the *Devices & networks* window.

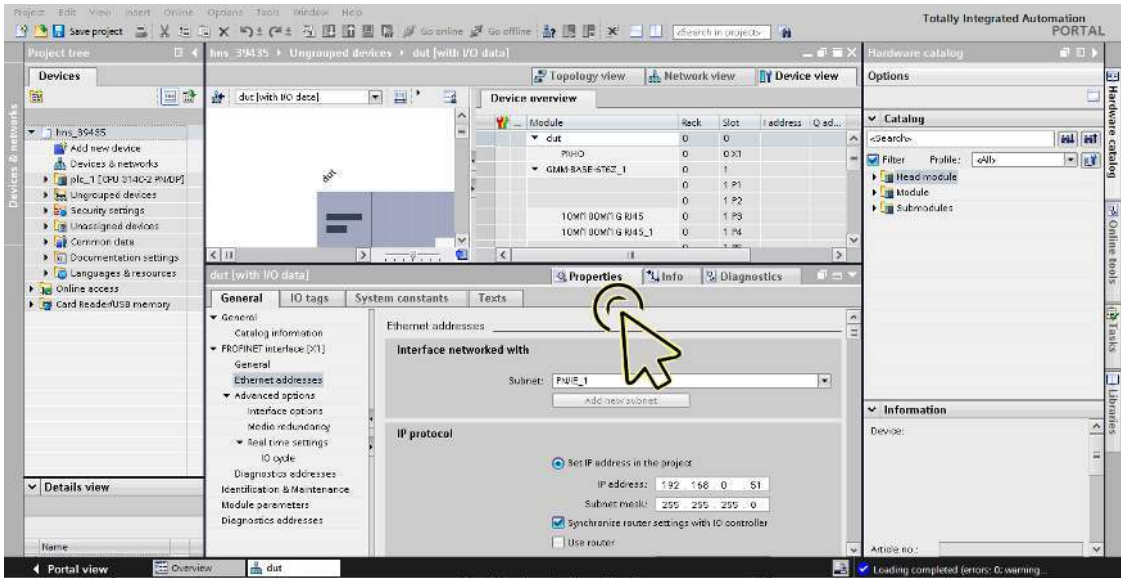
☐ In the *Network view* tab, click the icon of the device.



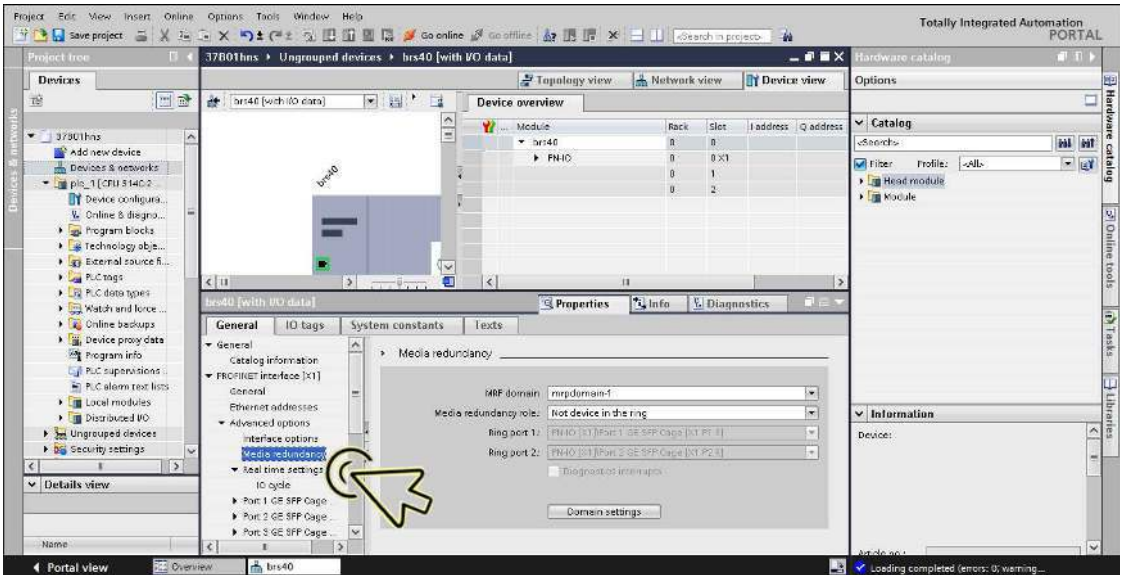
☐ Select the *Device view* tab to display the device details.



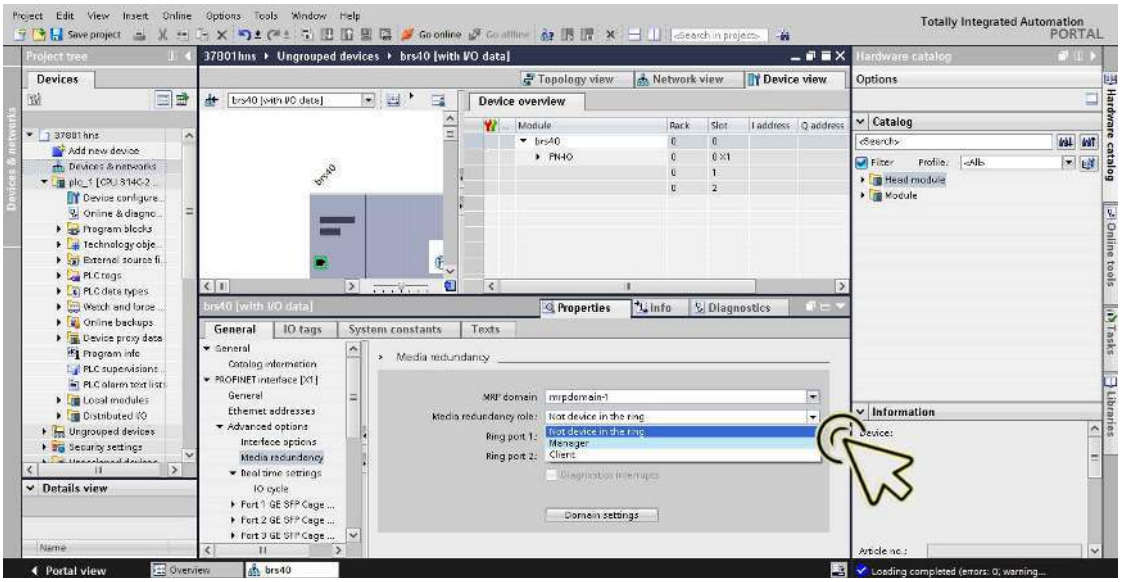
☐ Select the *Properties* tab.
The *Properties* tab contains additional tabs.



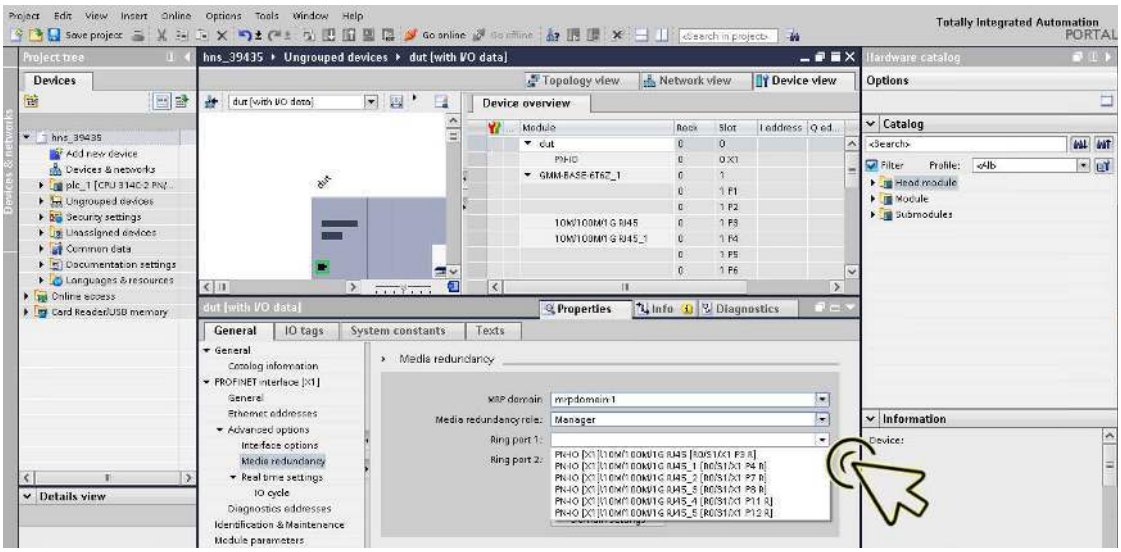
☐ In the *General* tab, navigate to the *PROFINET interface [X1] > Advanced options > Media redundancy* item.



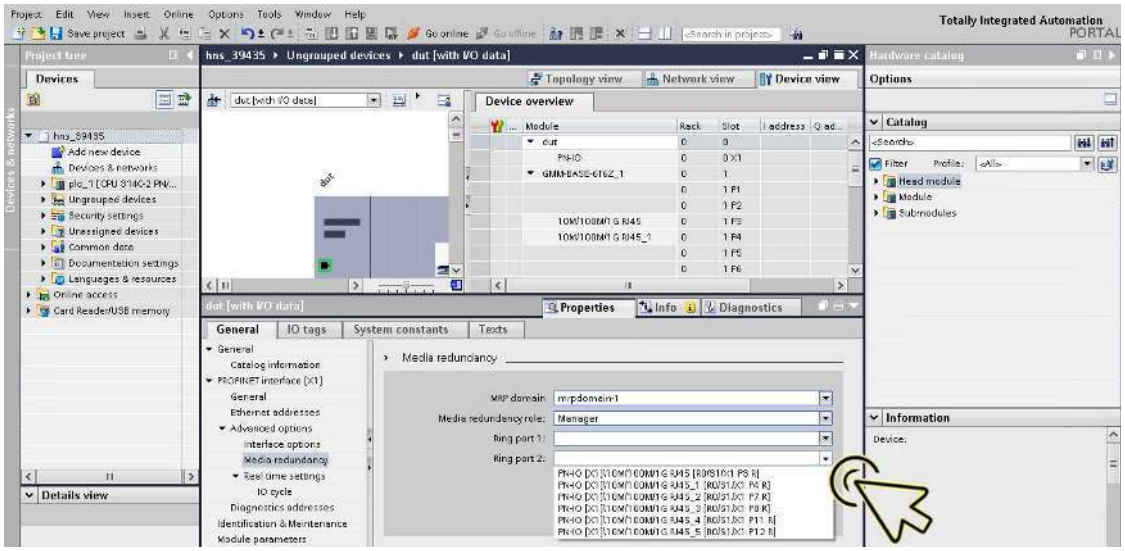
☐ From the *Media redundancy role* drop-down list, select the desired item.



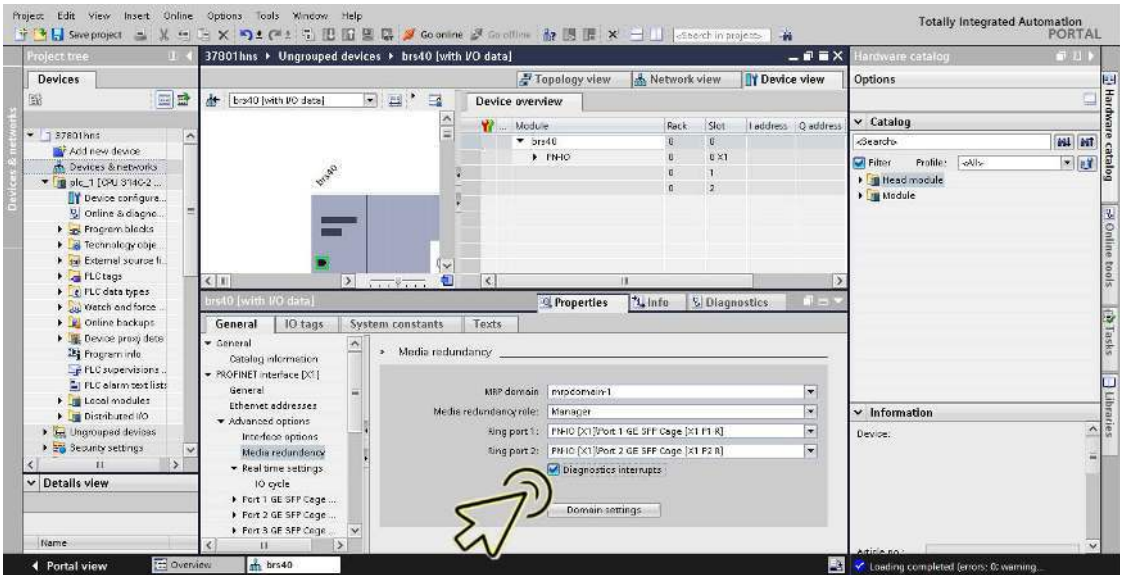
☐ From the *Ring port 1* drop-down list, select the desired item.



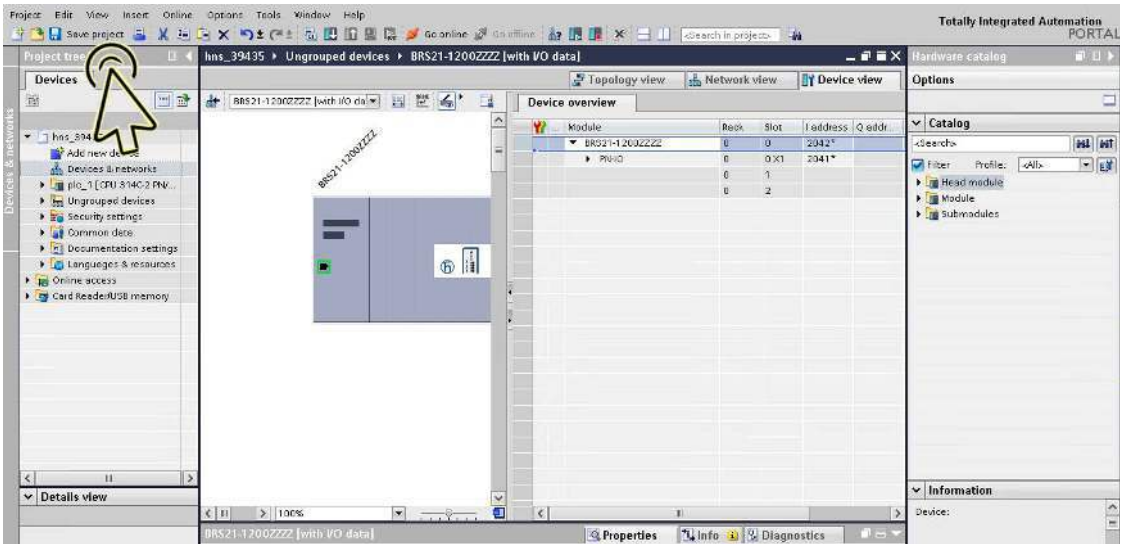
☐ From the *Ring port 2* drop-down list, select the desired item.



☐ Mark the *Diagnostics interrupts* checkbox to receive *MRP* ring `Open`/`Close` alarms.



☐ Click the *Save project* button.

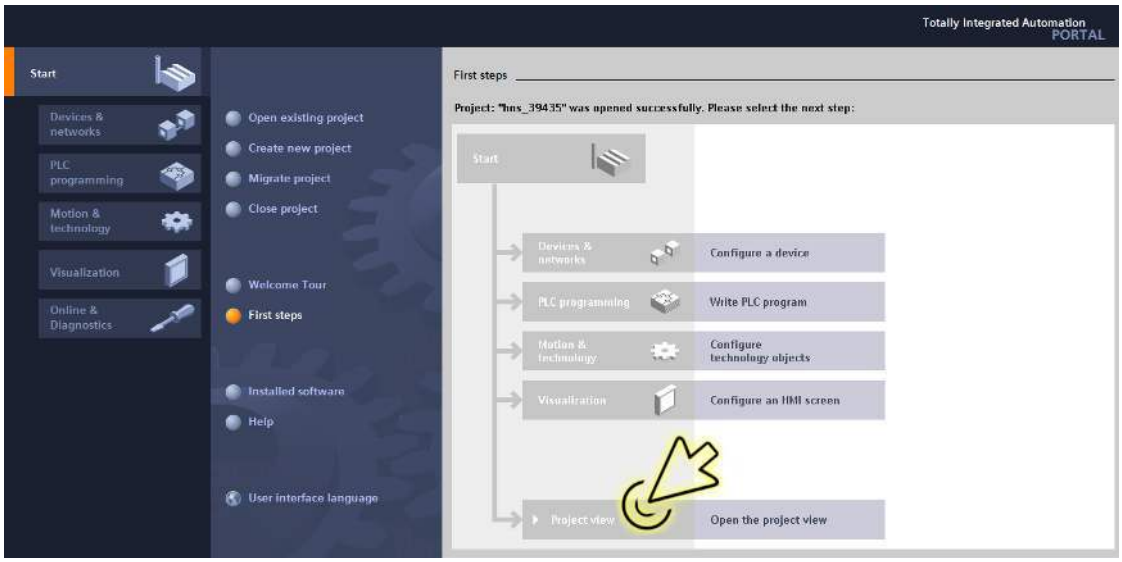


Note:
When an Application Relation is already established, do not disable any of the MRP Ring ports using the I/O modules (PROFINET).

Adding modules for modular devices

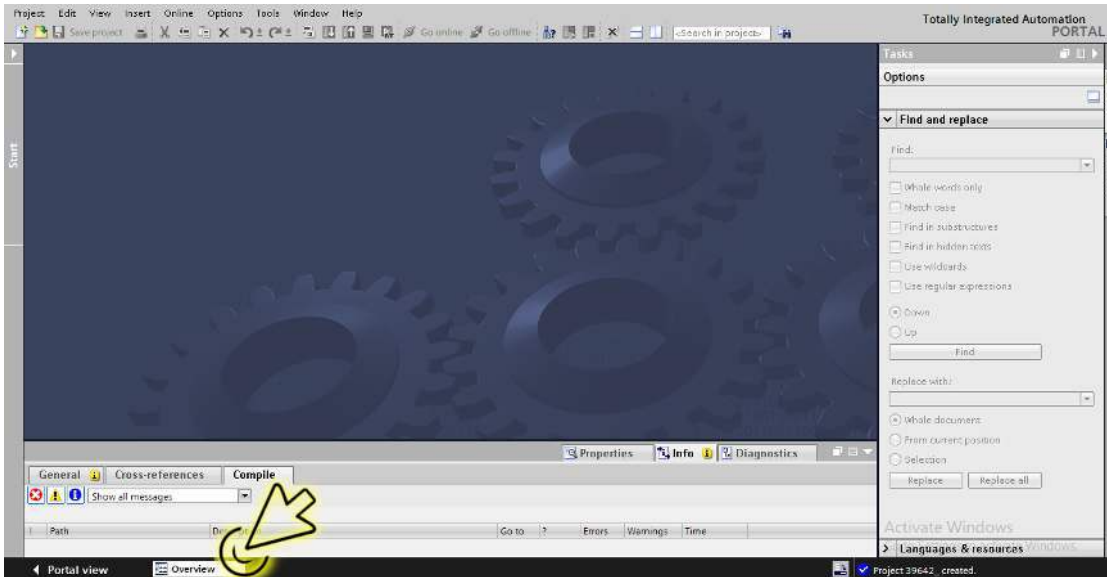
Perform the following steps:

☐ Click the *Project view* icon.



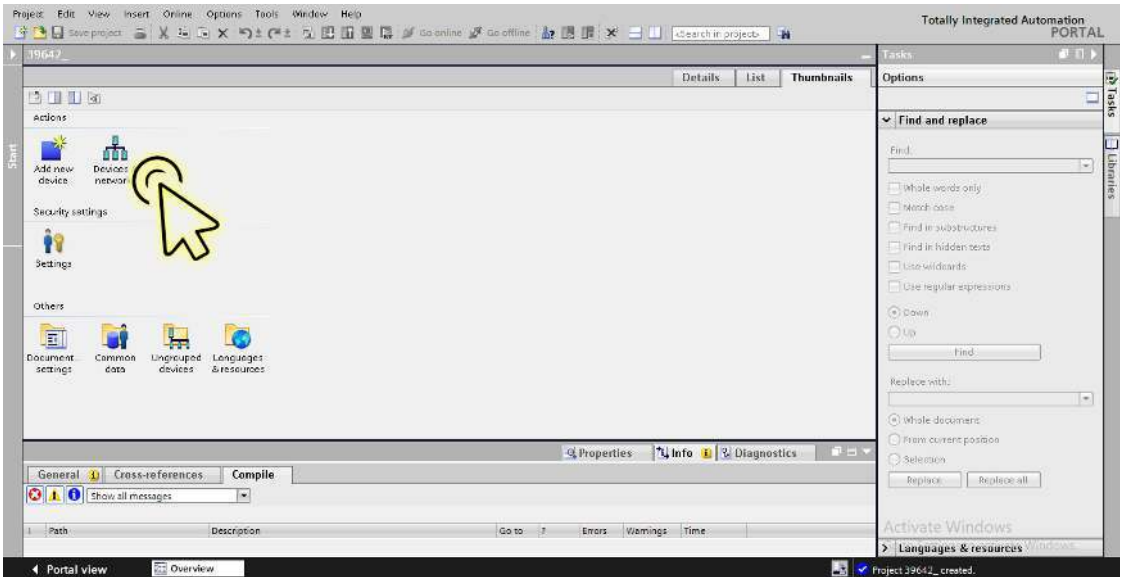
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



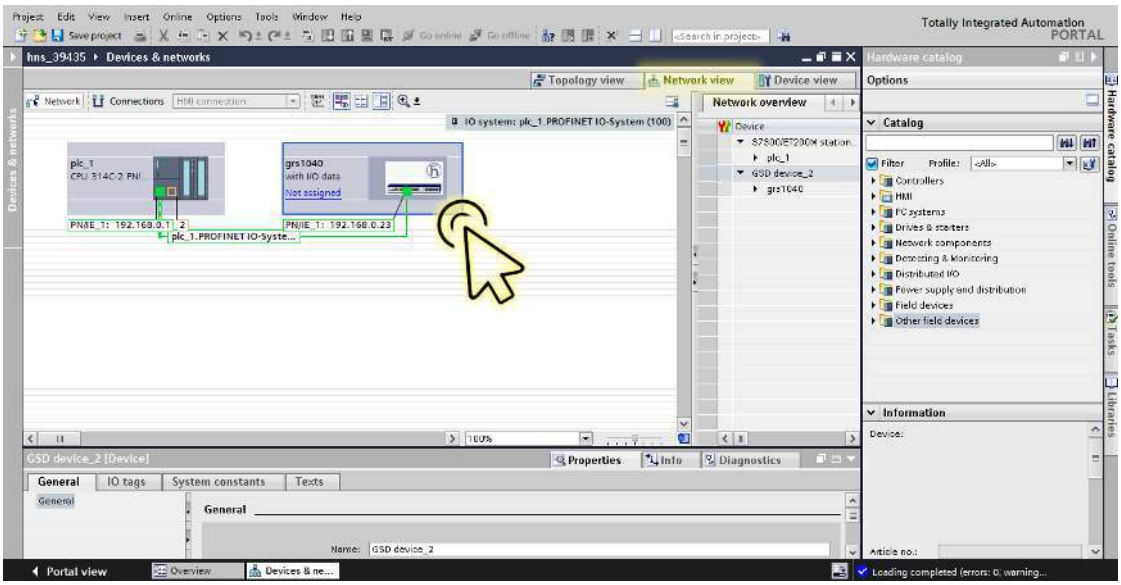
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

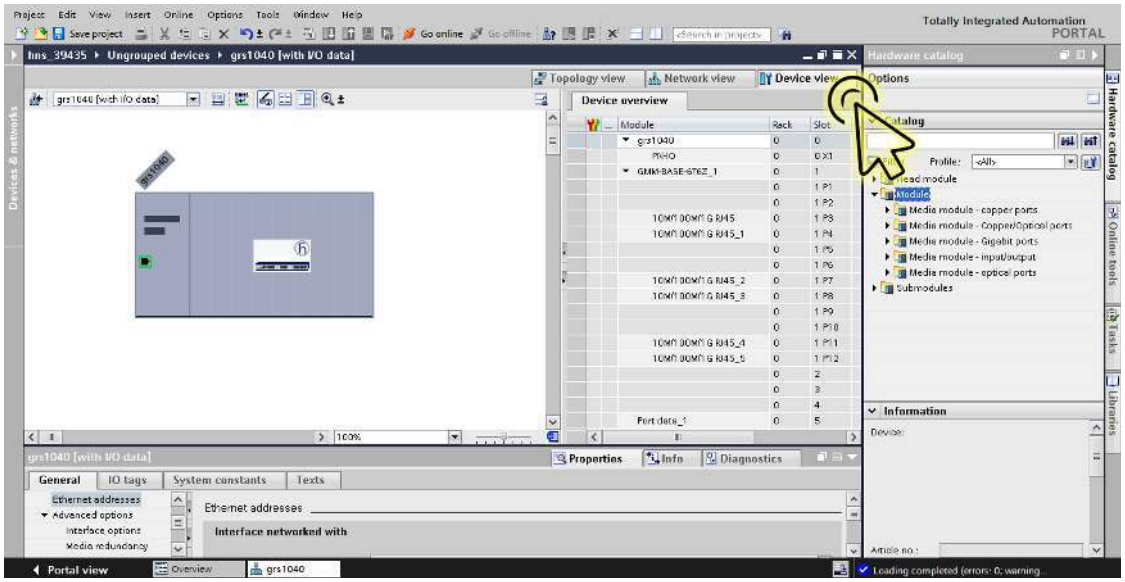


The dialog displays the *Devices & networks* window.

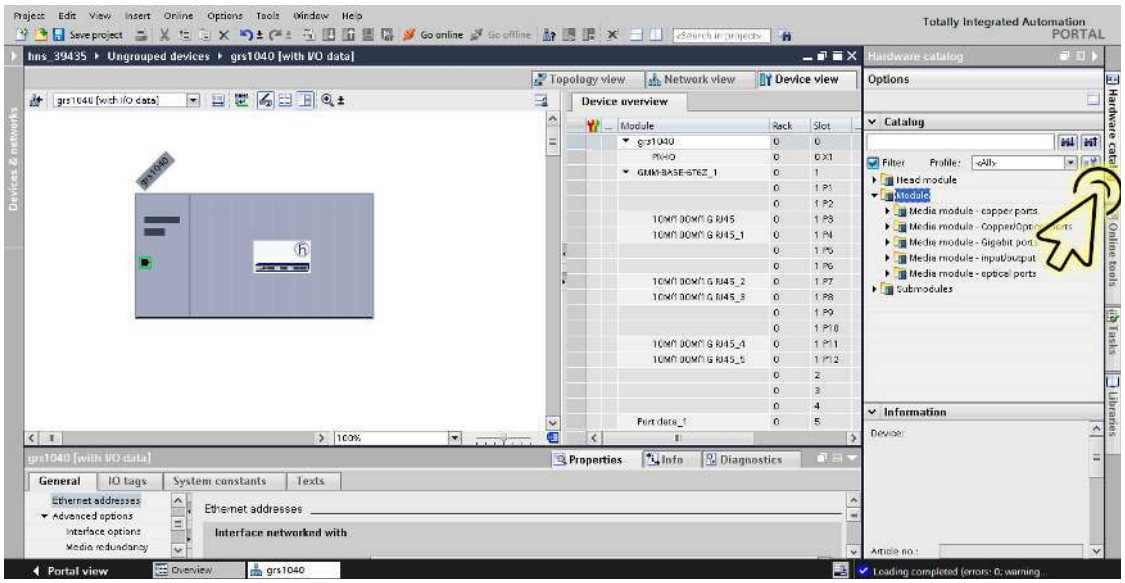
☐ Select the *Network view* tab.
☐ Click the icon of the device that is under test.



☐ Select the *Device view* tab to display the device details.

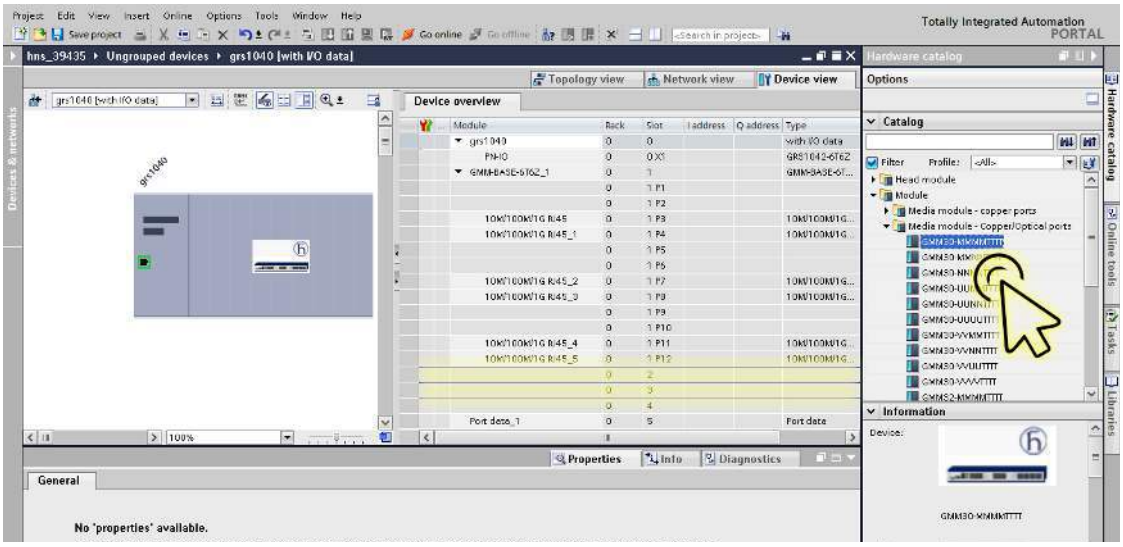


☐ Select the *Hardware catalog* tab in the right margin to display the *Catalog* pod.



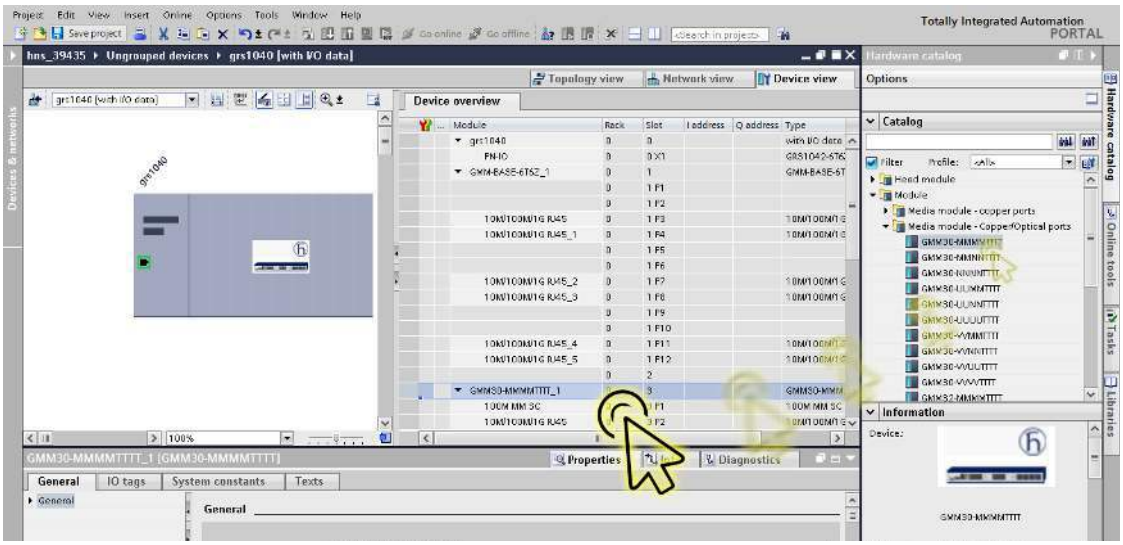
The tree view displays the available media modules.

☐ In the tree view, select the required module.



In the *Device view* tab, the slot which is physically connected to the device is highlighted.

☐ Drag the selected module, and drop it onto the highlighted slot in the *Device view* tab.

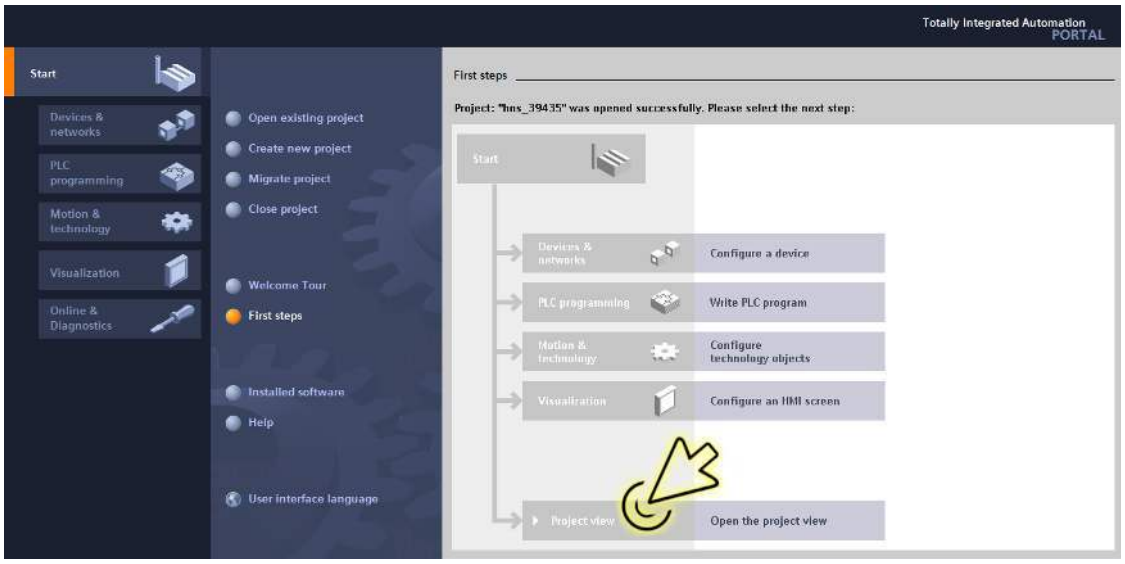


Note:
The TIA Portal automatically adds the *fixed ports* when you add a module in the *Device view* tab. If the module has SFP slots, you need to set up the SFPs. See section “Adding an SFP transceiver as a submodule in non-modular devices” on page 348.

Adding digital I/O modules in non-modular devices

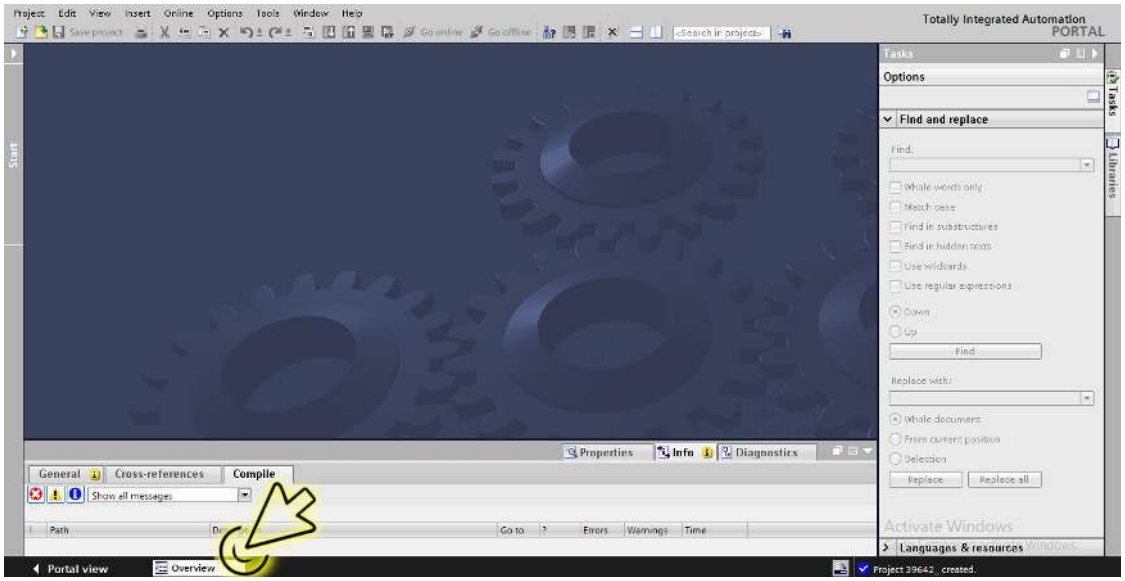
In non-modular devices, *device data* modules and *port data* modules are available that transfer the I/O data packets in the *PROFINET* network. For inserting a *device data* module or *port data* module, perform the following steps:

☐ Click the *Project view* icon.



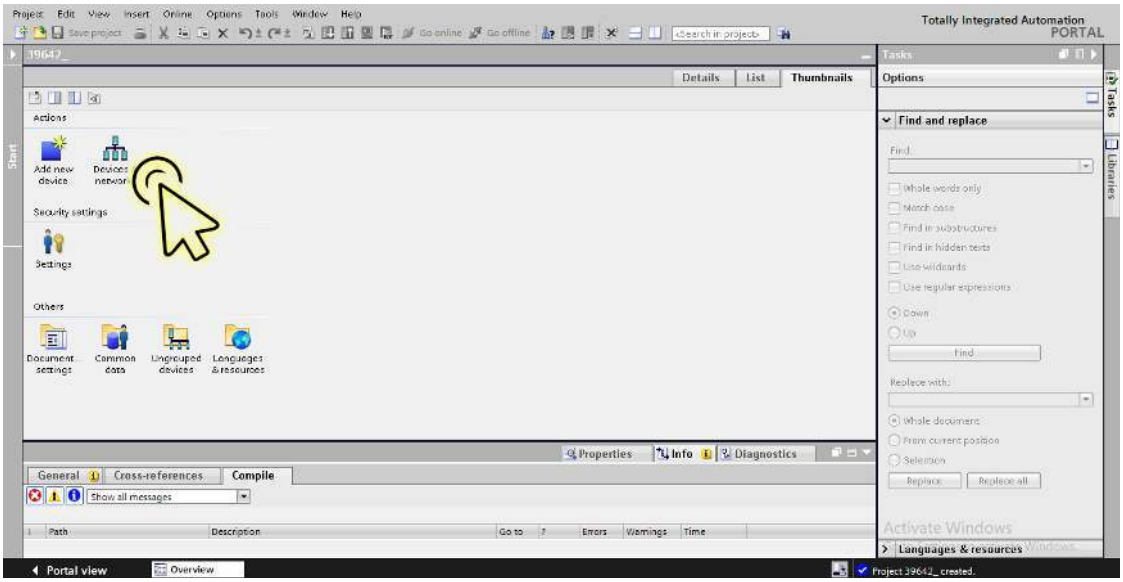
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



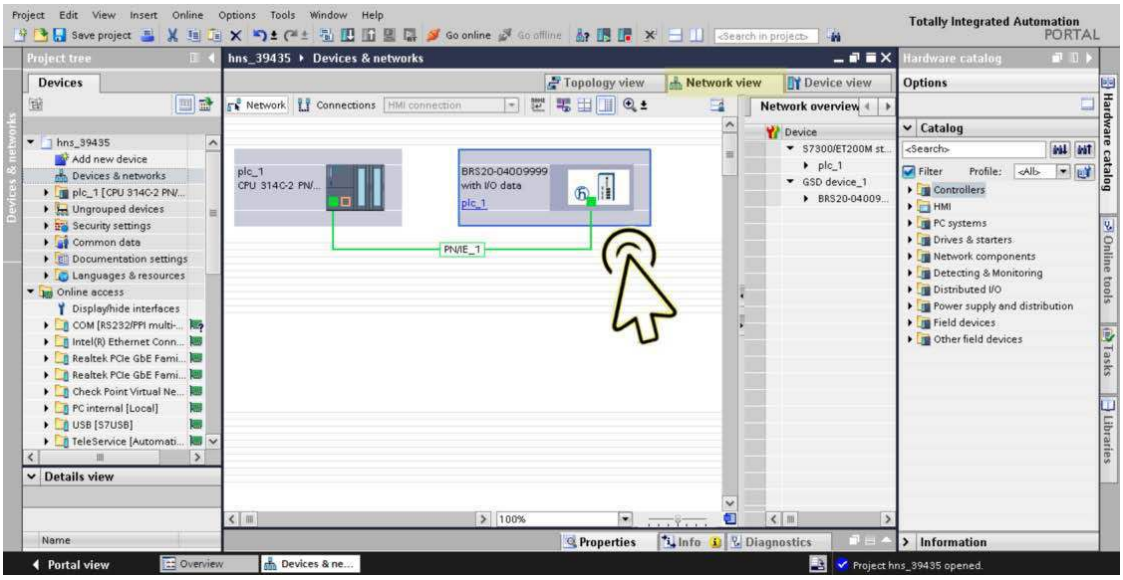
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

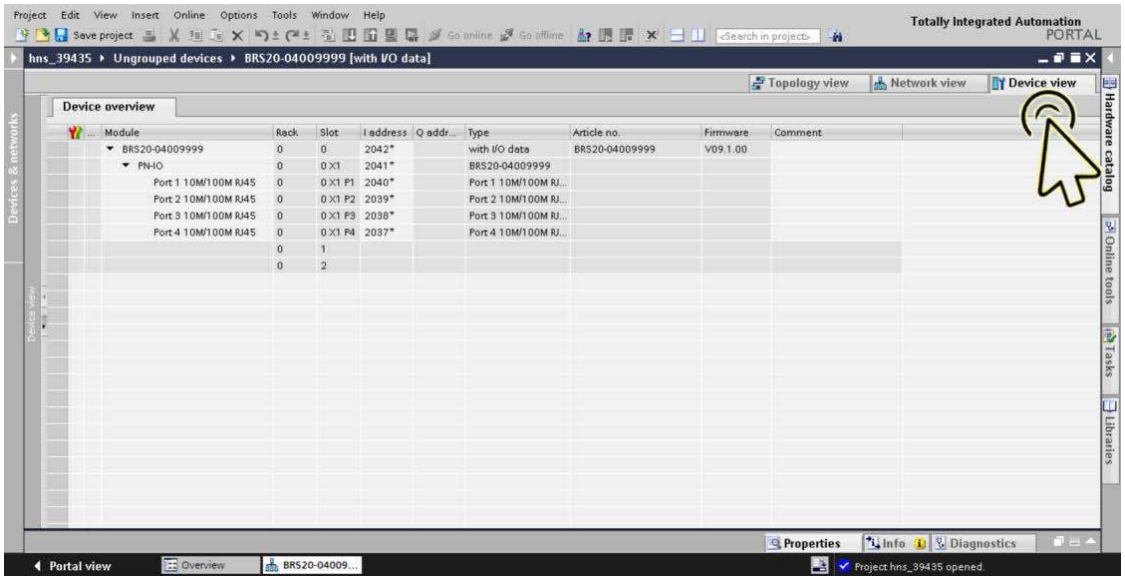


The dialog displays the *Devices & networks* window.

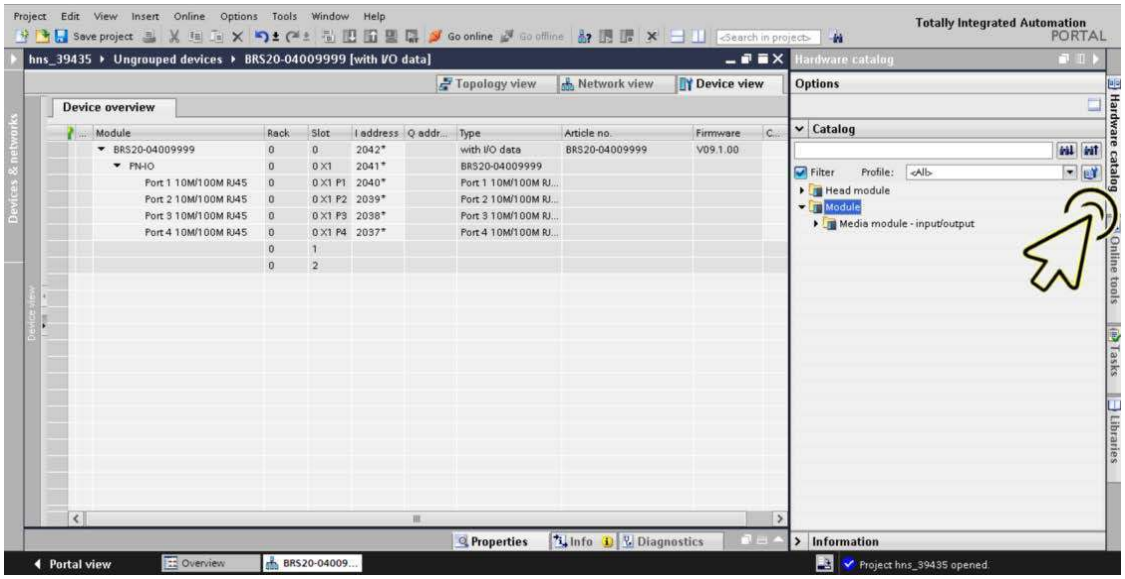
☐ In the *Network view* tab, click the icon of the device.



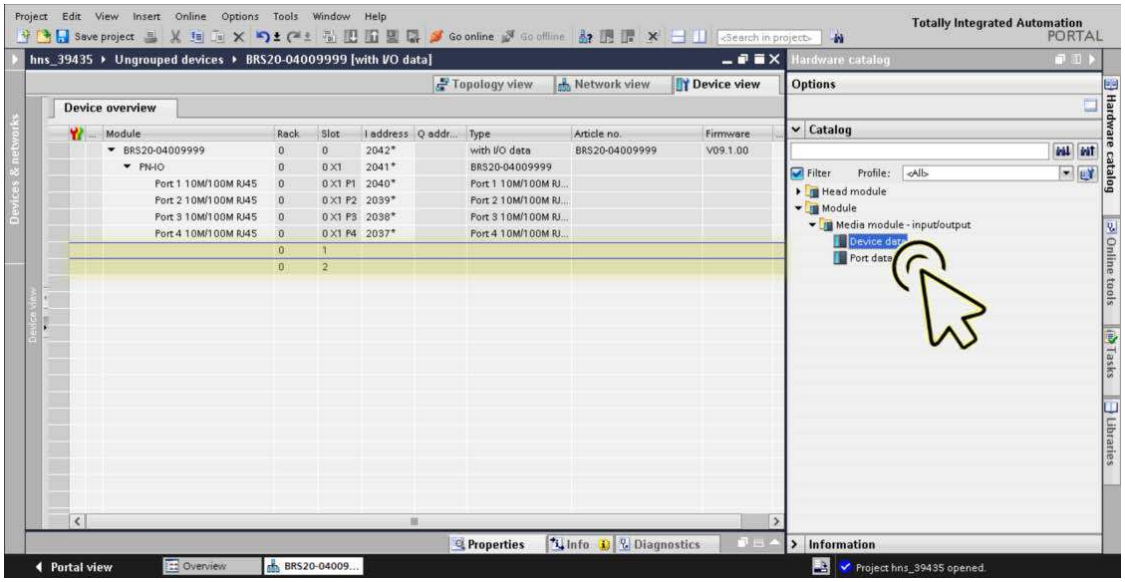
☐ Select the *Device view* tab to display the device details.



☐ Select the *Hardware catalog* tab in the right margin to display the available media modules.

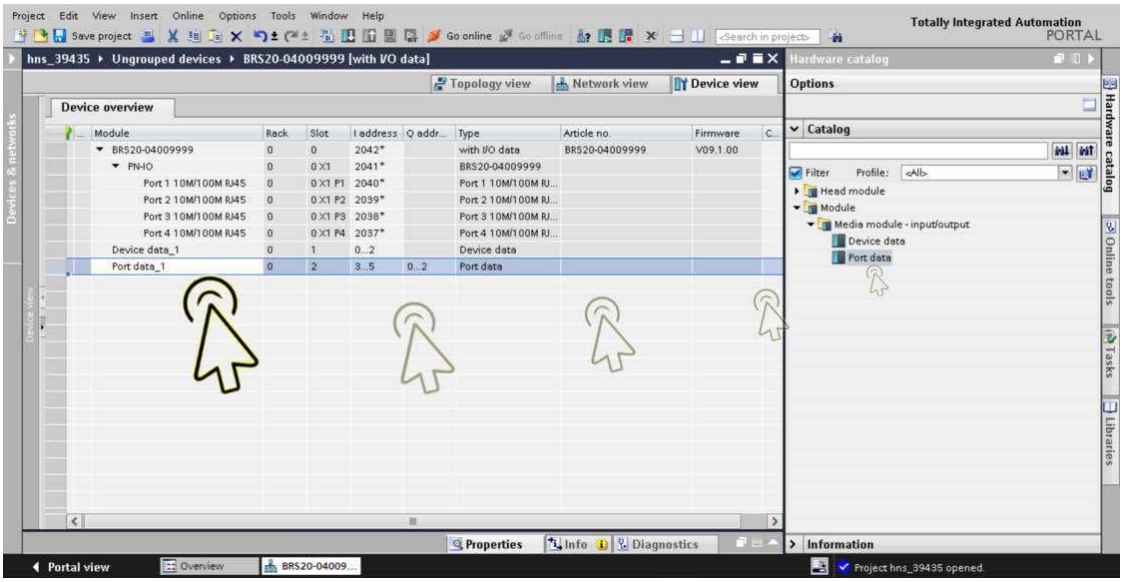


☐ Select the required *Device data* module or *Port data* module.

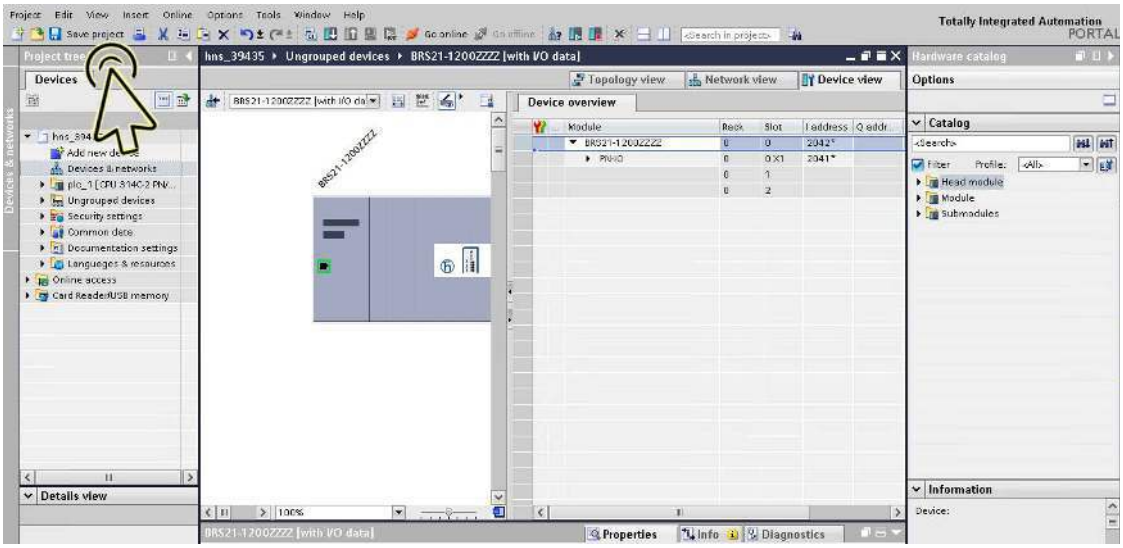


In the *Device view* tab, the slot which is logically connected to the device is highlighted.

☐ Drag the selected module, and drop it onto the highlighted slot in the *Device view* tab.



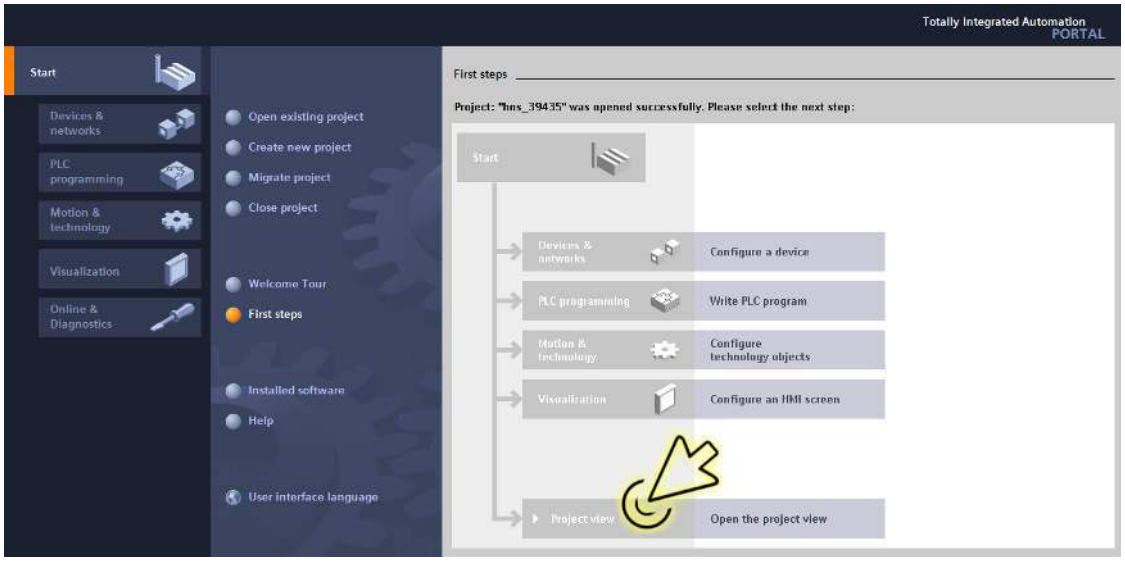
☐ Click the *Save project* icon.



Adding digital I/O modules in modular devices

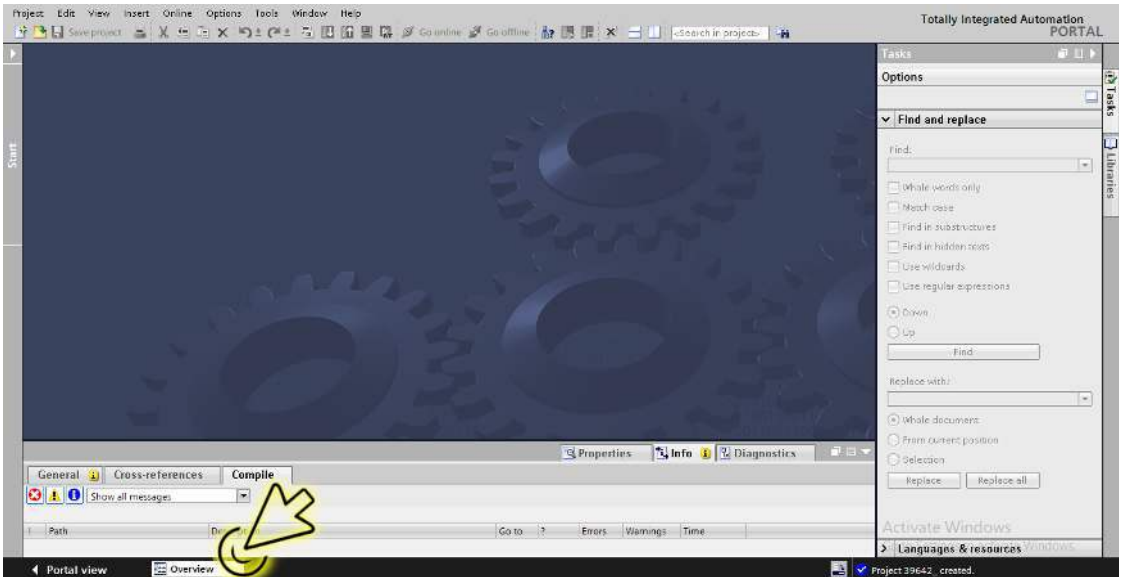
In modular devices, *device data* modules and *port data* modules are available that transfer the I/O data packets in the *PROFINET* network. For inserting a *device data* module or *port data* module, perform the following steps:

☐ Click the *Project view* icon.



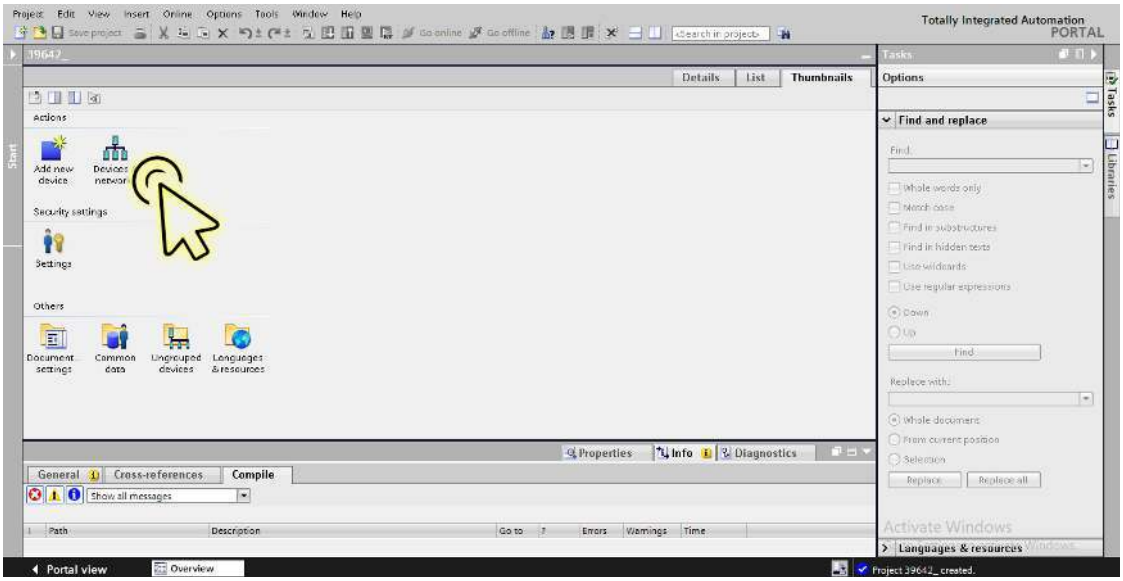
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



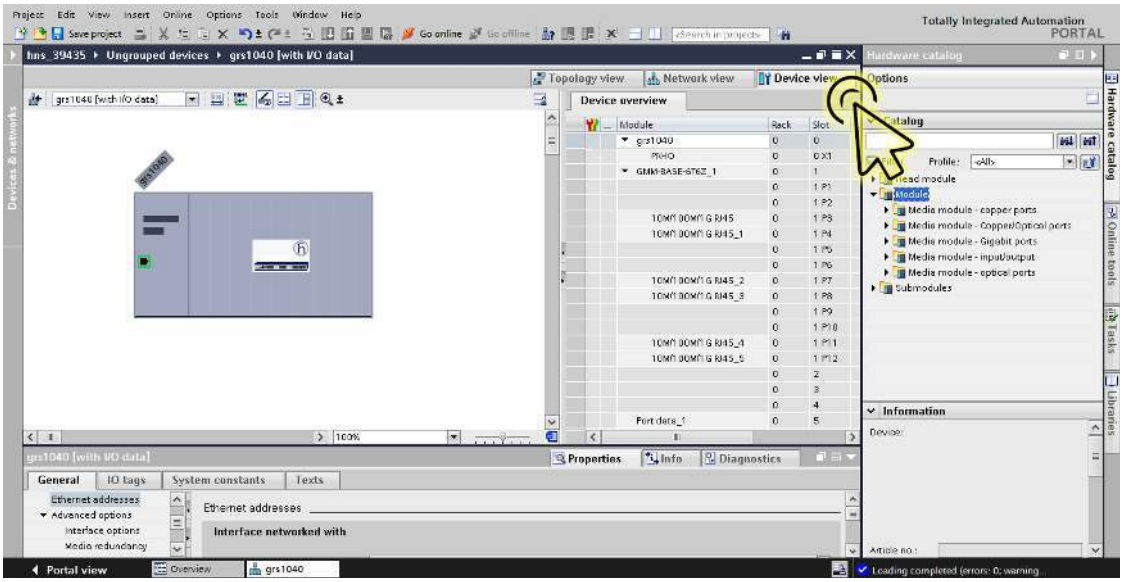
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

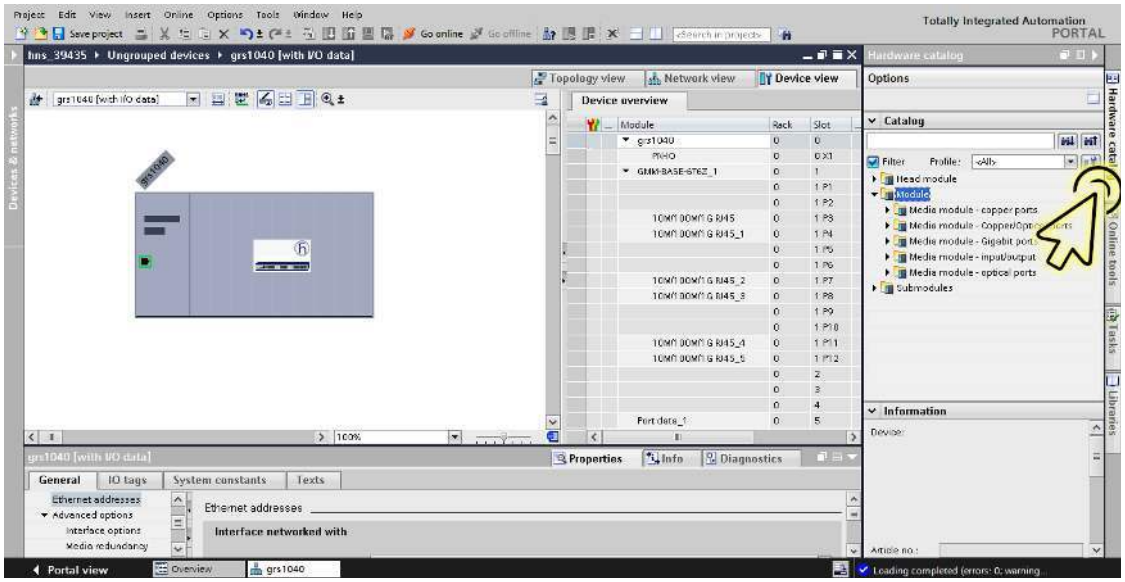


The dialog displays the *Devices & networks* window.

☐ Select the *Device view* tab to display the device details.

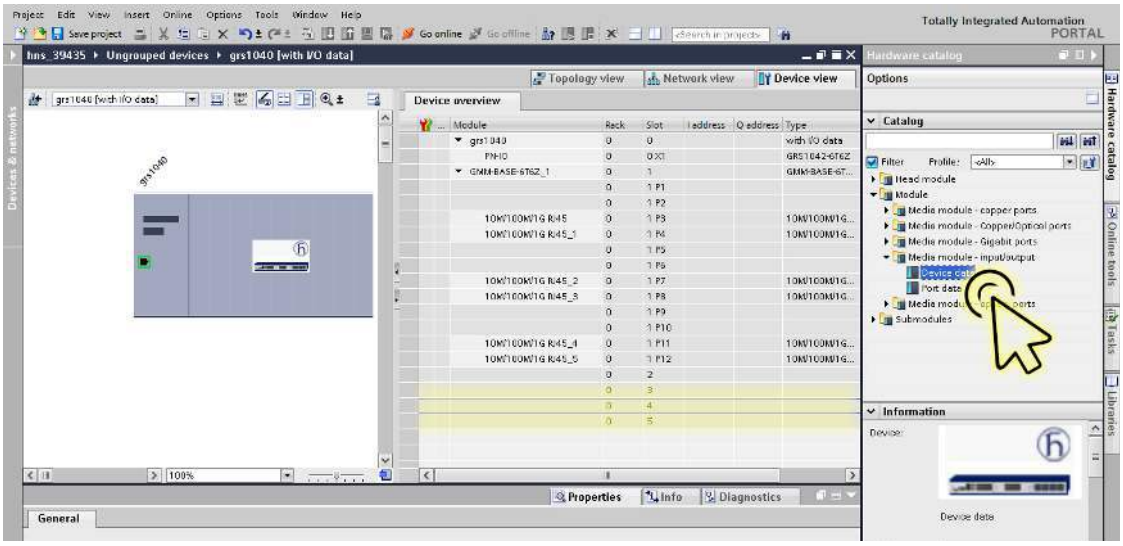


☐ Select the *Hardware catalog* tab in the right margin to display the *Catalog* pod.



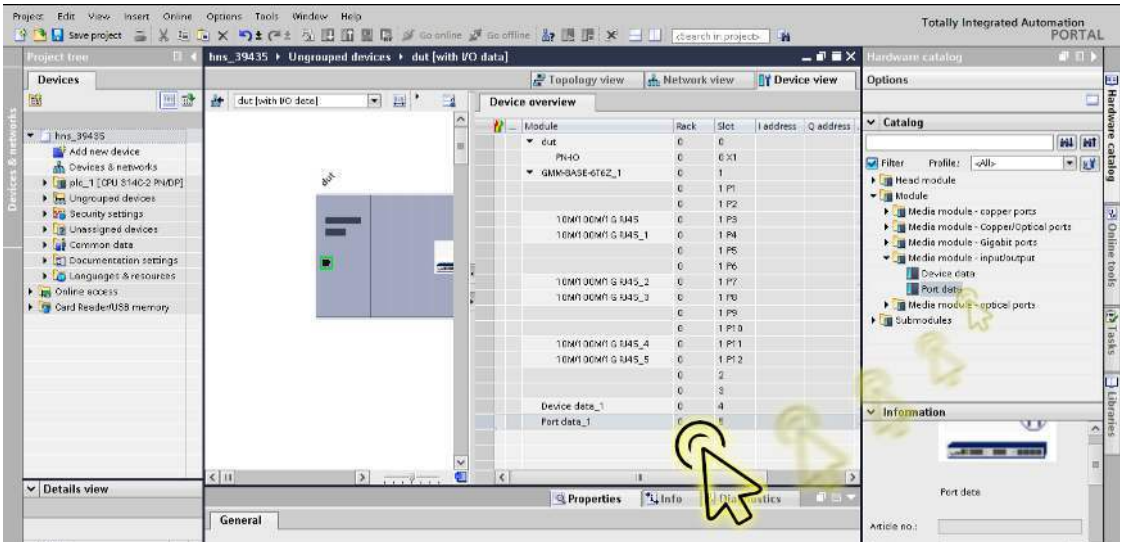
The tree view displays the available media modules.

☐ In the tree view, *Media module - input/output* branch, select the required *device data* module or *port data* module.



In the *Device view* tab, the slot which is logically connected to the device is highlighted.

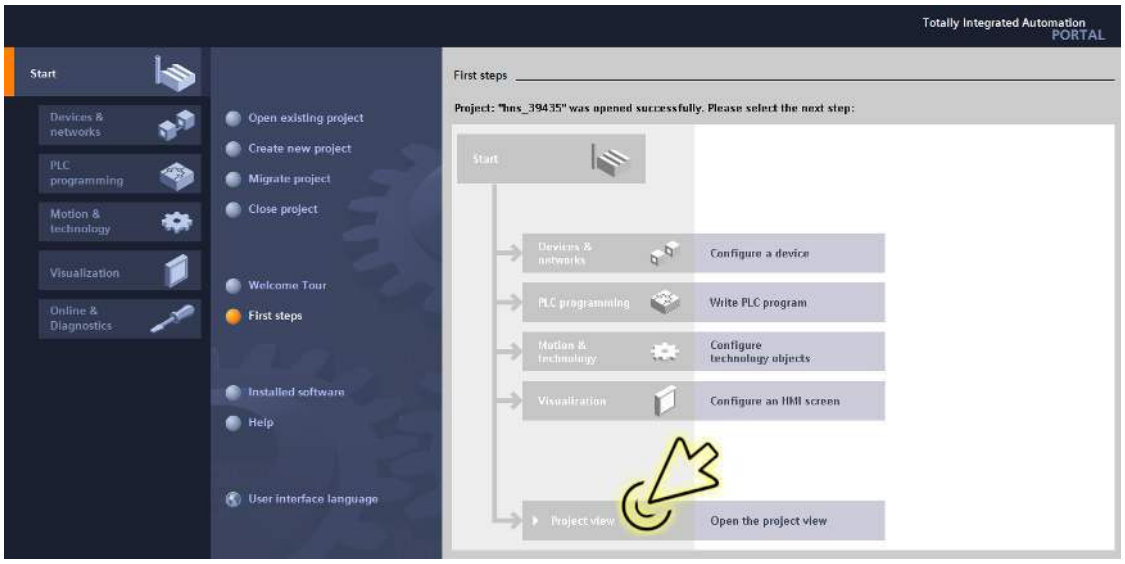
☐ Drag the selected module, and drop it onto the highlighted slot in the *Device view* tab.



Adding an SFP transceiver as a submodule in non-modular devices

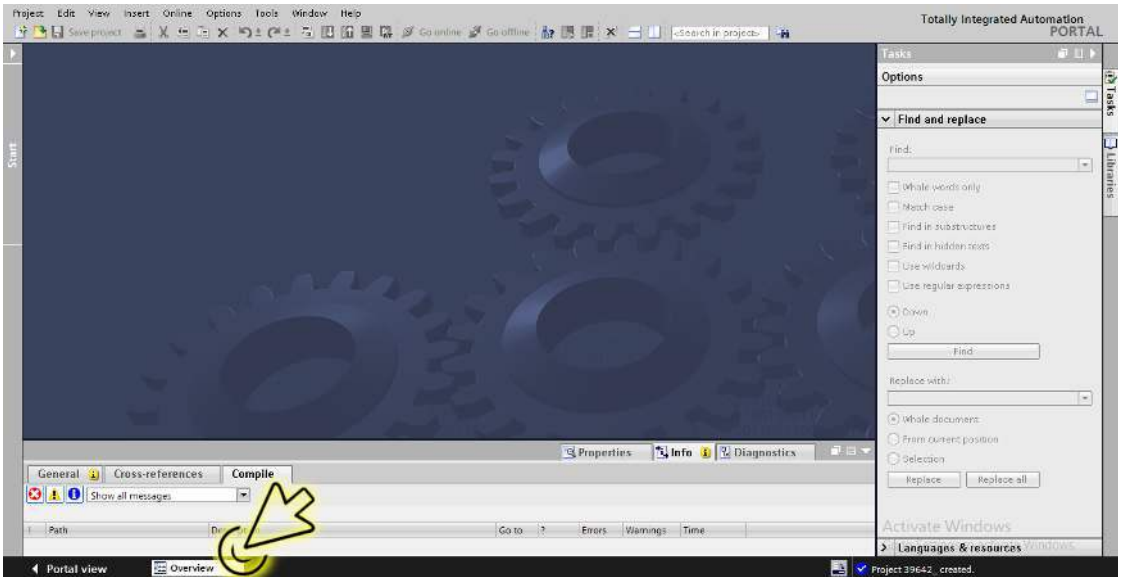
In the TIA Portal, you can set up SFP (Small Form-factor Pluggable) transceivers as submodules in the free SFP slots of the device representation. To set up an SFP submodule, perform the following steps:

☐ Click the *Project view* icon.



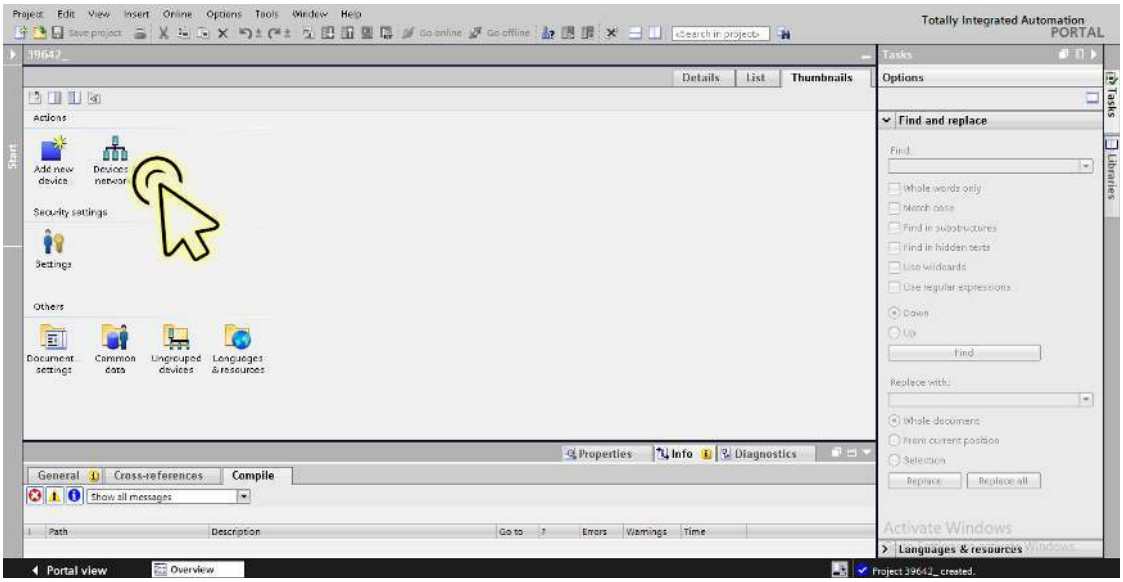
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



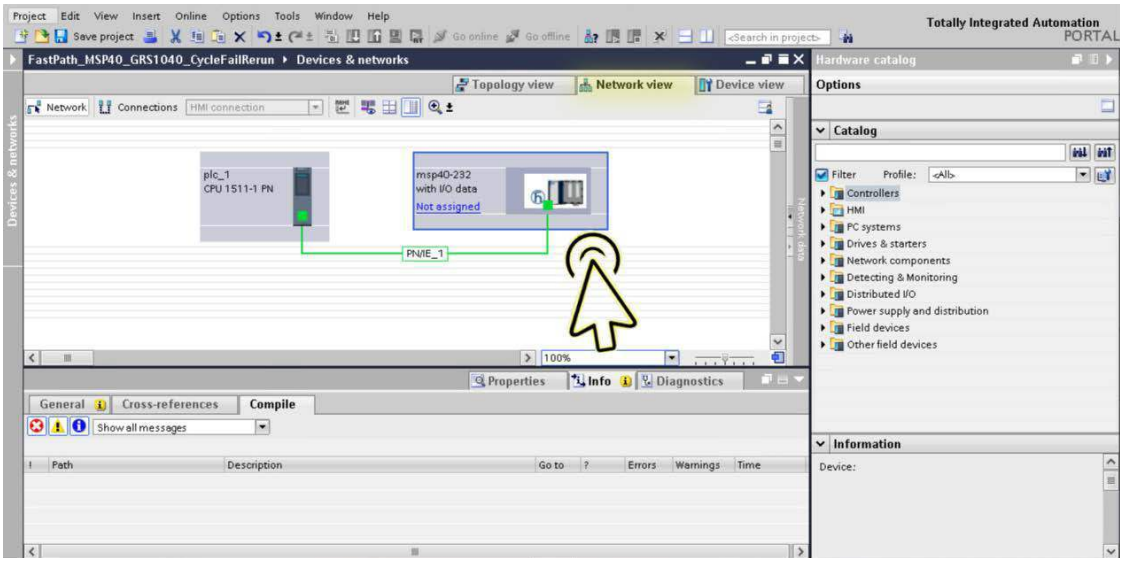
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

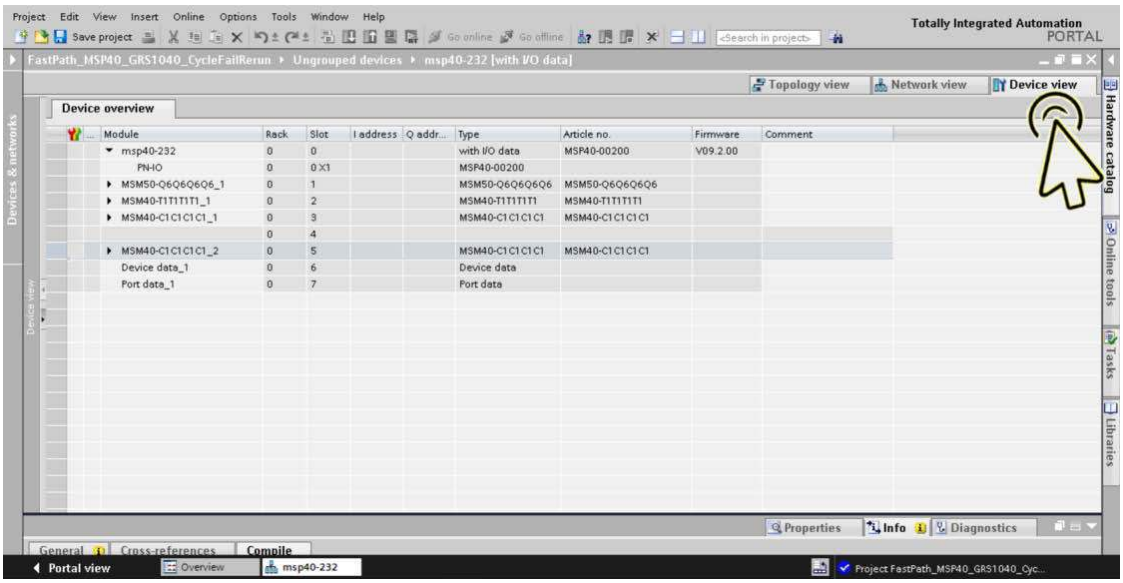


The dialog displays the *Devices & networks* window.

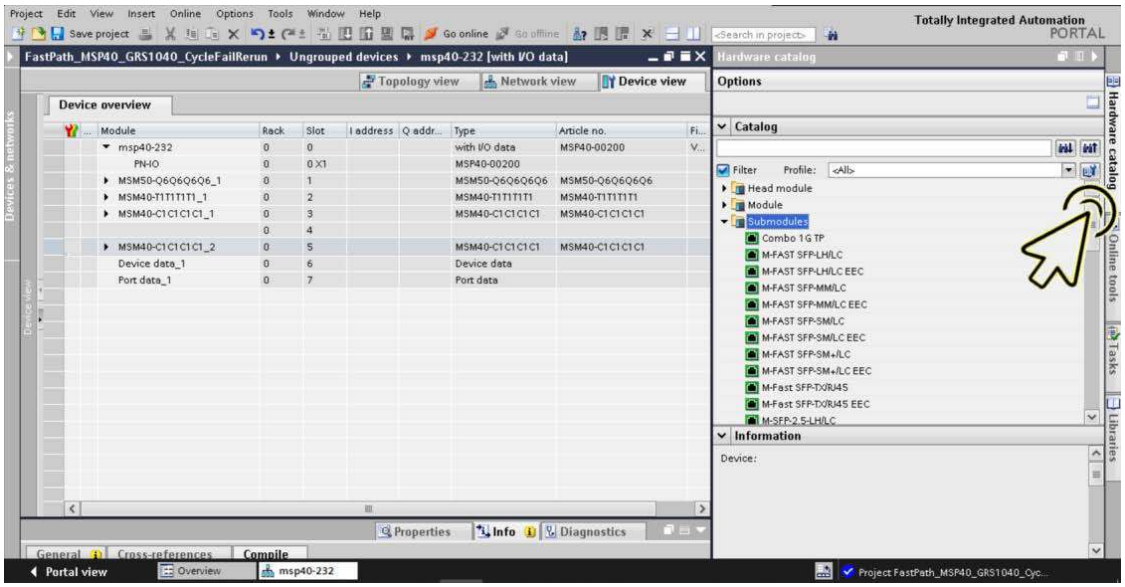
☐ In the *Network view* tab, click the icon of the device.



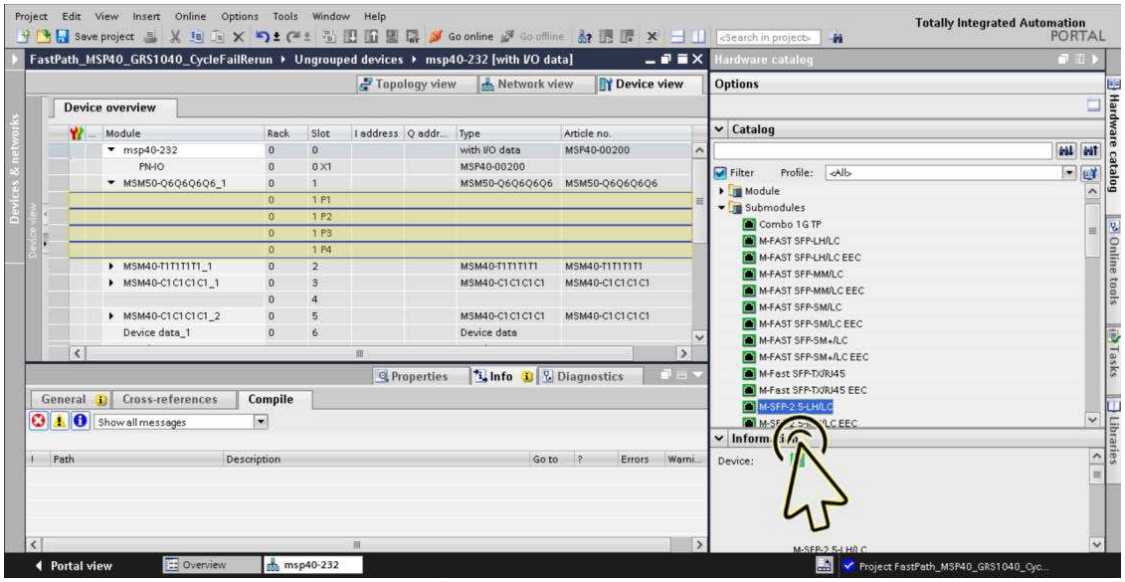
☐ Select the *Device view* tab to display the device details.



☐ Select the *Hardware catalog* tab in the right margin to display the available SFP submodules.

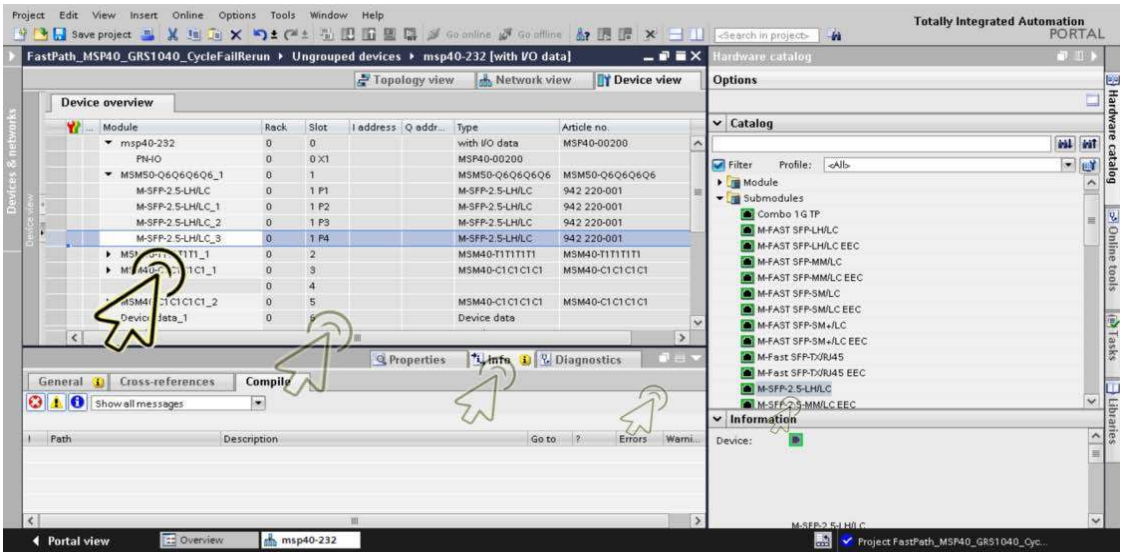


☐ Select the required SFP submodule.

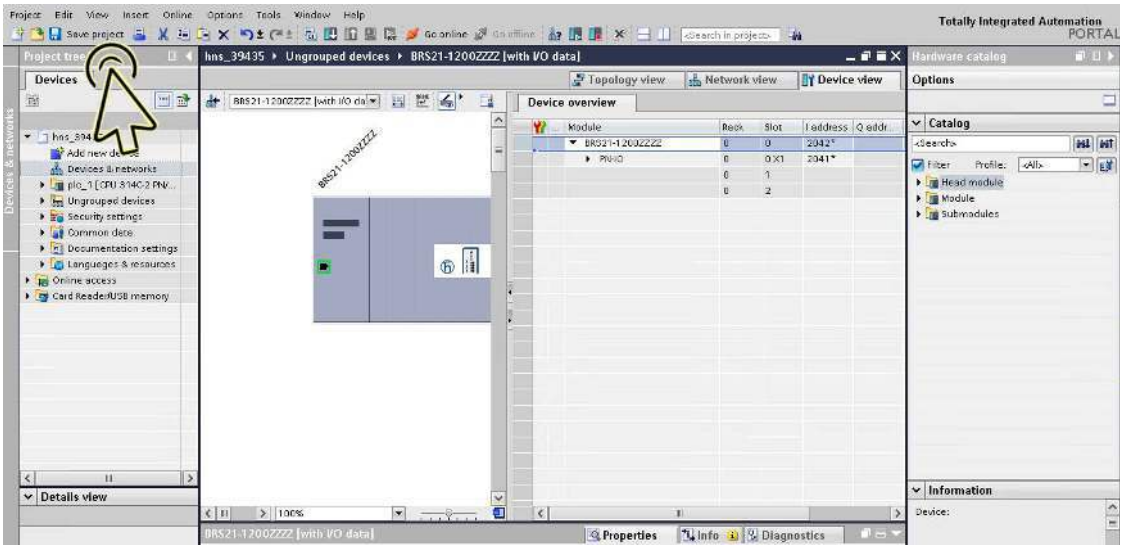


In the *Device view* tab, the slot which is logically connected to the device is highlighted.

☐ Drag the selected SFP submodule, and drop it onto the highlighted slot in the *Device view* tab.



☐ Click the *Save project* icon.



Note:
Verify that the SFP submodule you added in the TIA Portal and the physically connected SFP submodule are of the same type. Otherwise, the Application Relation may not be set up correctly.

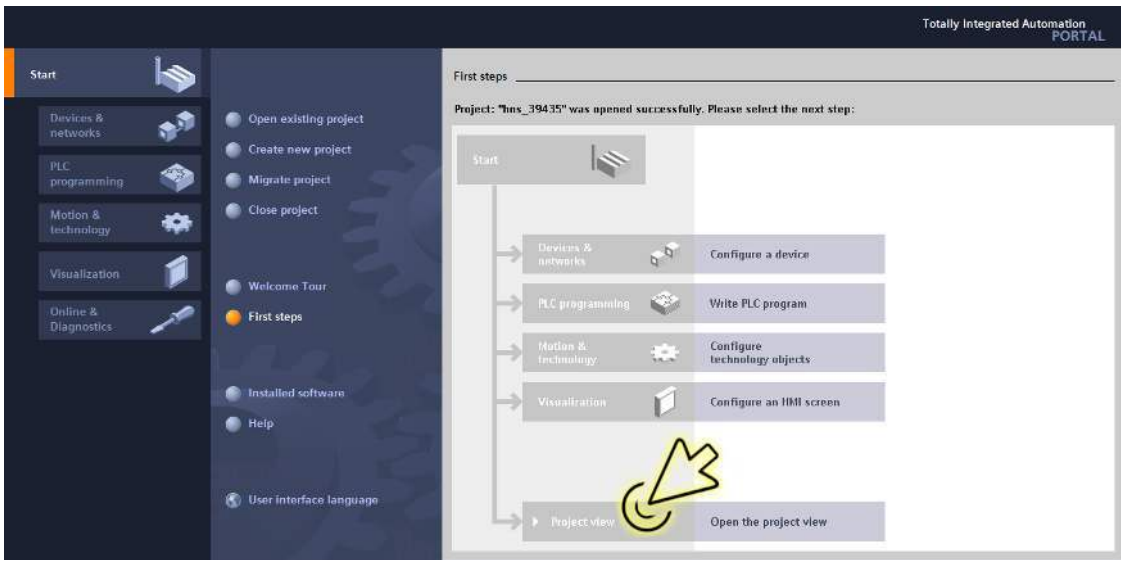
Configuring the port properties

In a modular device with n I/O modules, the I/O modules are represented by the slots 1 through n. The ports of a particular I/O module are represented by subslots in the respective slot. The *device data* module is represented by the next to last slot (n+1) and the *port data* module is represented by the last slot (n+2).

A non-modular device with n ports only has the slot 0. The ports are represented as subslots 1 through n in slot 0. The *device data* module is represented by the next to last subslot (n+1) and the *port data* module is represented by the last subslot (n+2).

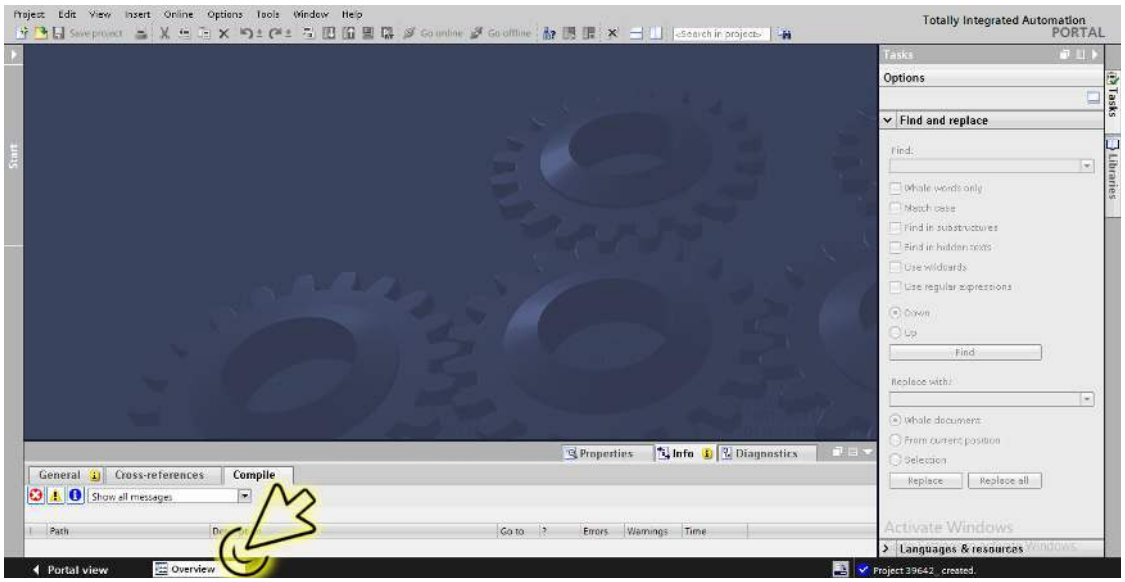
Set up the port link monitoring alarm. To do this, perform the following steps:

☐ Click the *Project view* icon.



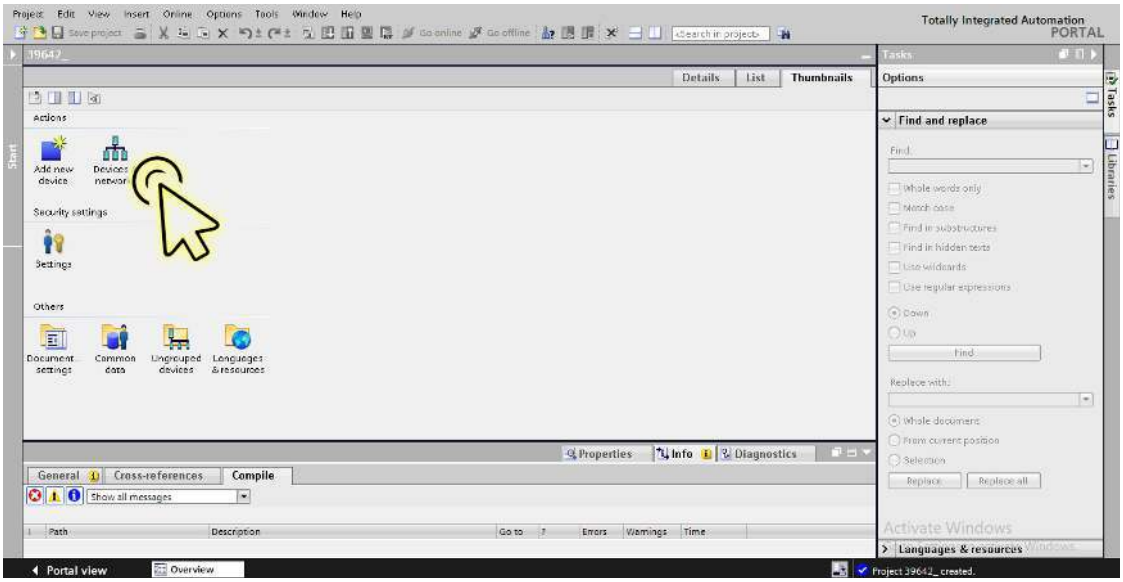
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



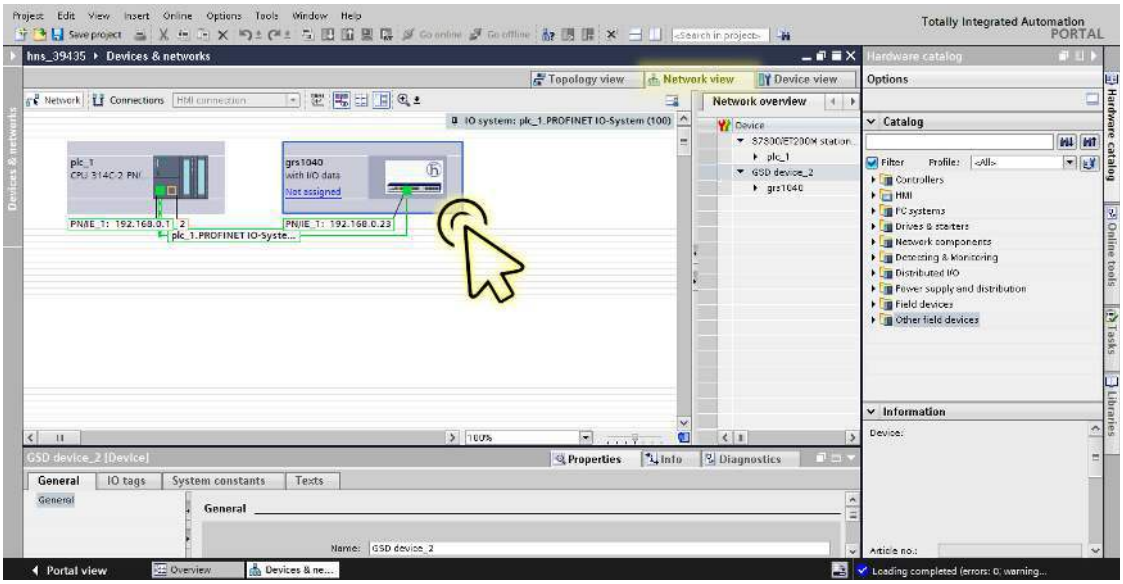
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

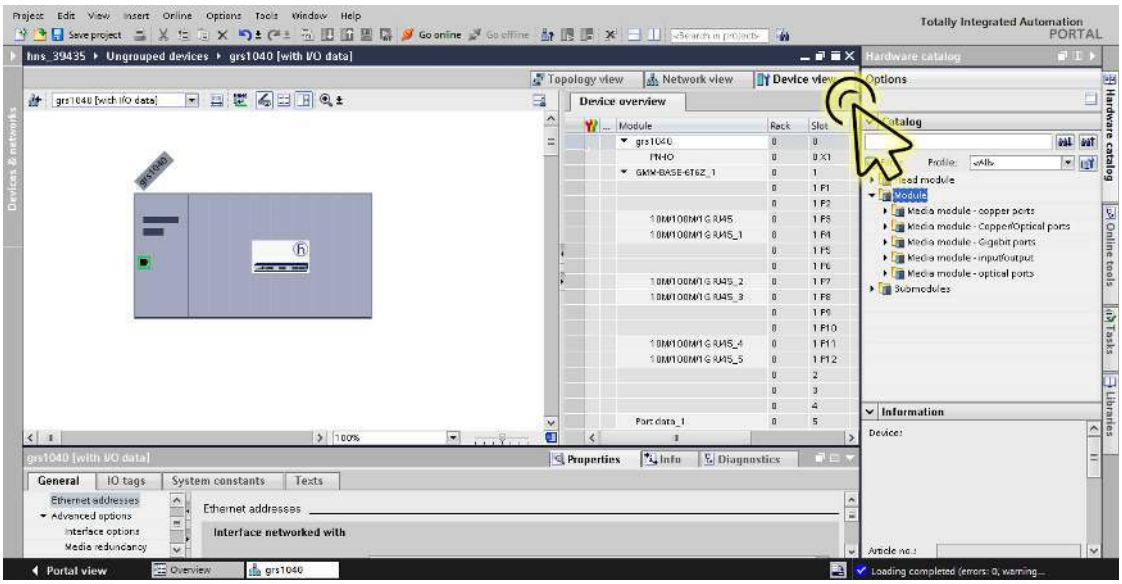


The dialog displays the *Devices & networks* window.

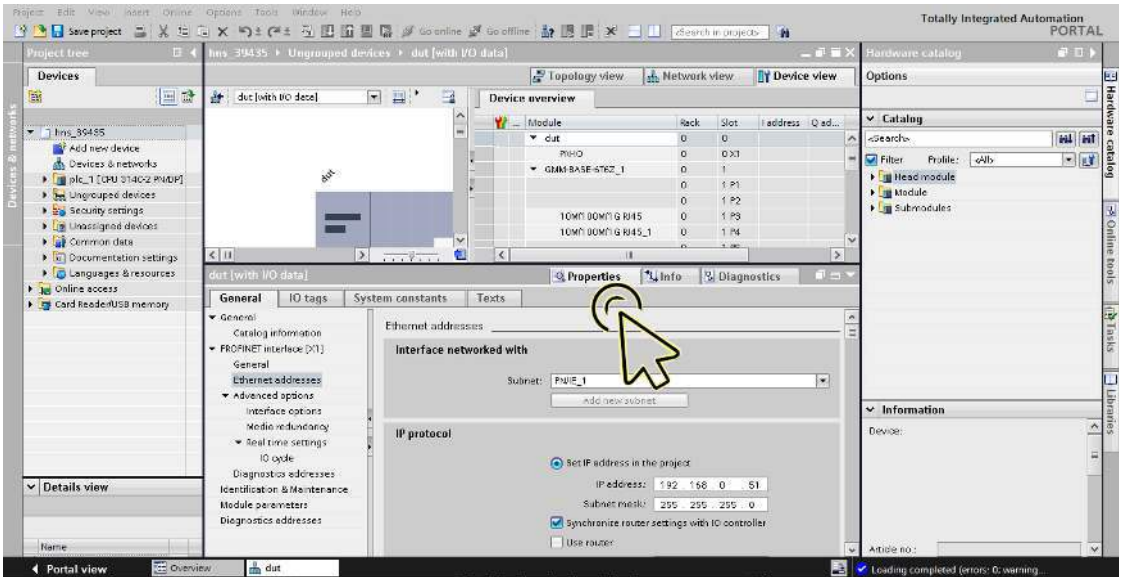
☐ In the *Network view* tab, click the icon of the device.



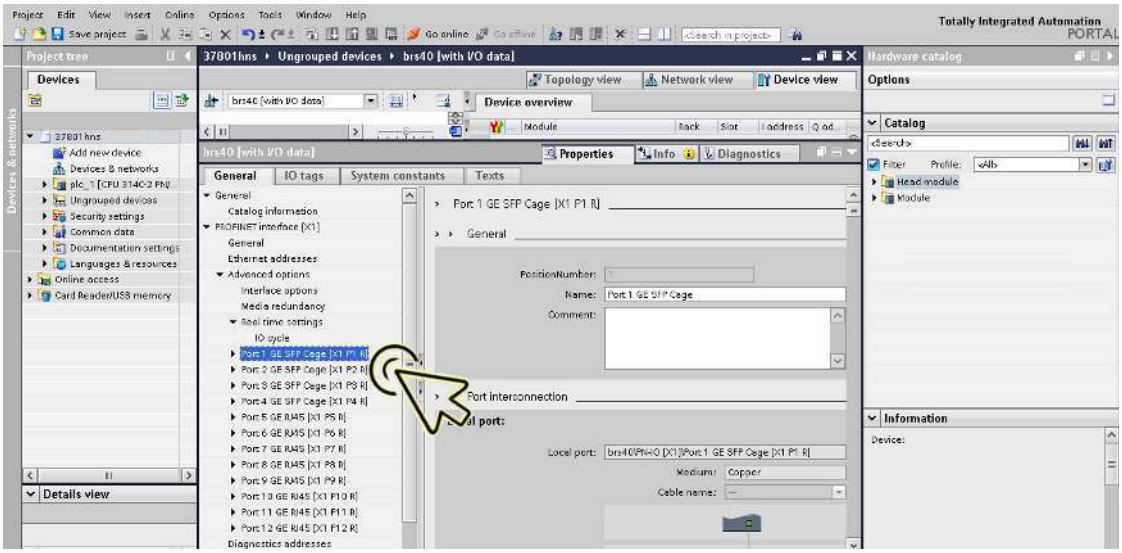
☐ Select the *Device view* tab to display the device details.



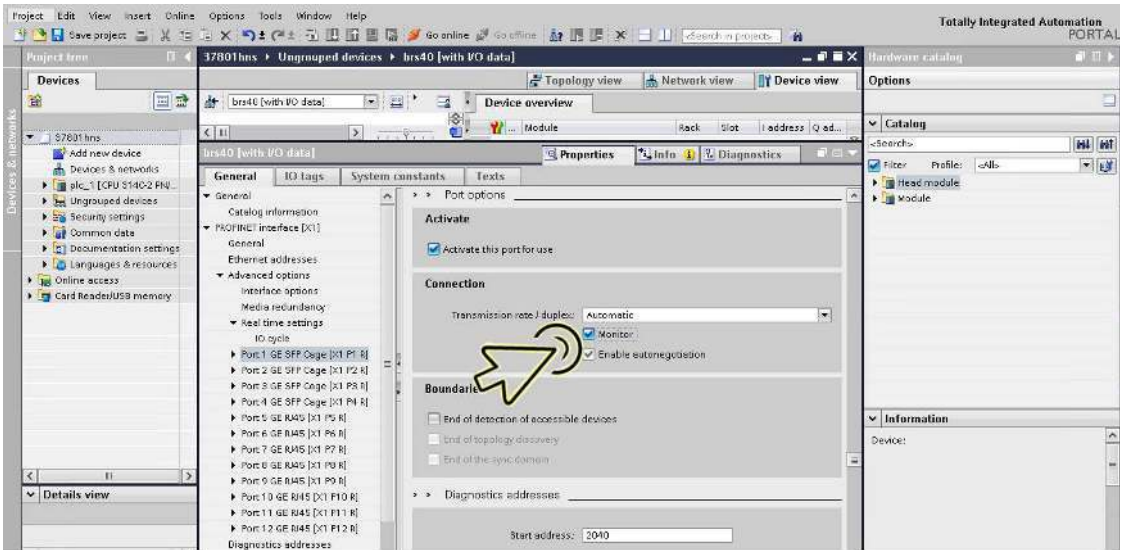
☐ Select the *Properties* tab.
The *Properties* tab contains additional tabs.



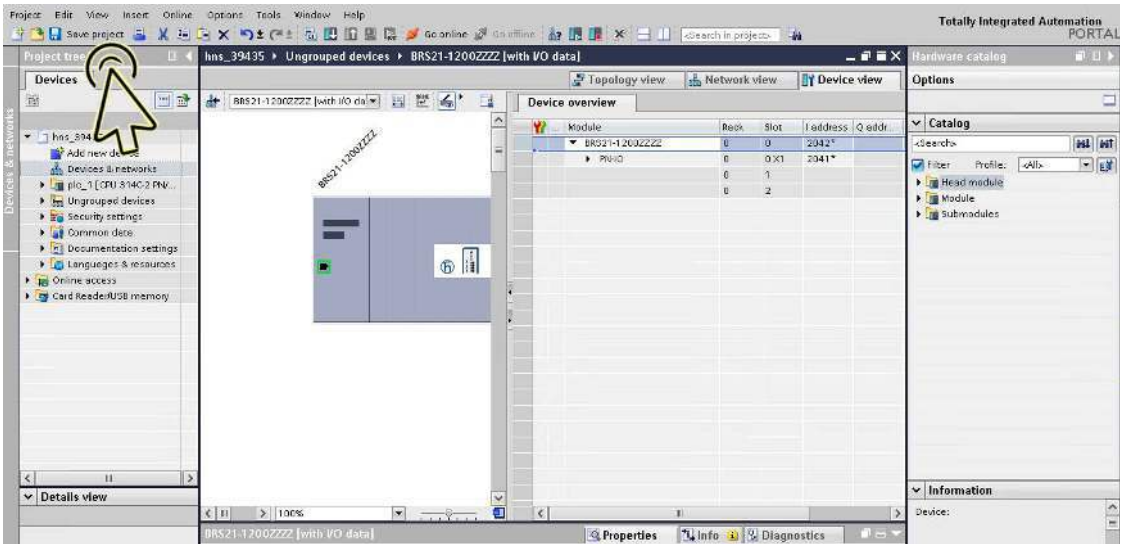
☐ In the *General* tab, navigate to the *PROFINET interface [X1] > Advanced options* item, then click the required port.



☐ In the *Port options* section, *Connection* frame, mark the *Monitor* checkbox.



☐ Click the *Save project* button.

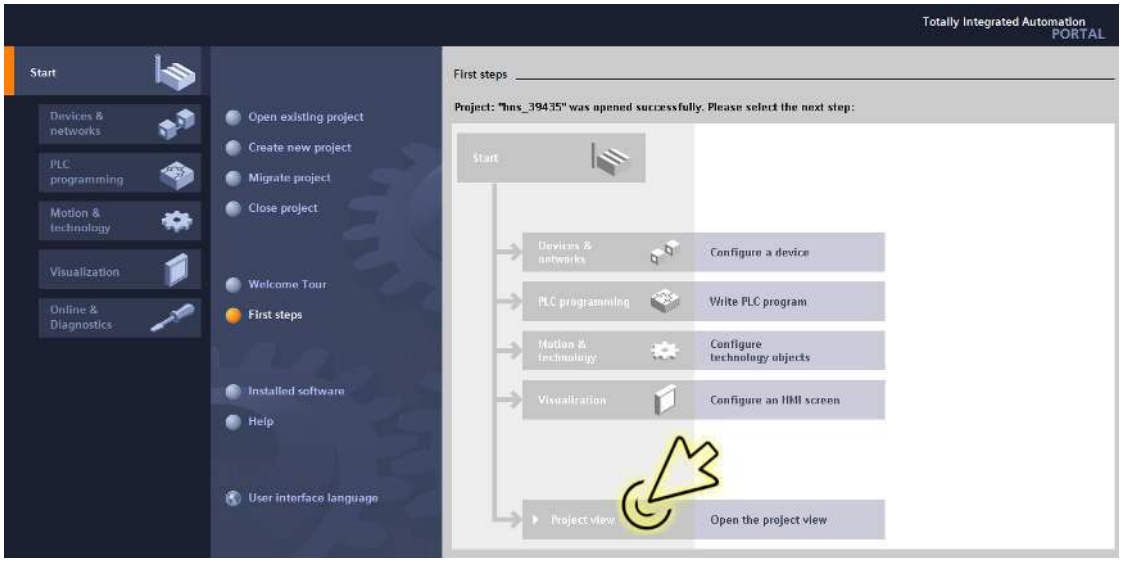


Note:
To test the port link monitor function, you can temporarily unplug the data cable from the respective port.

Configuring the connection options

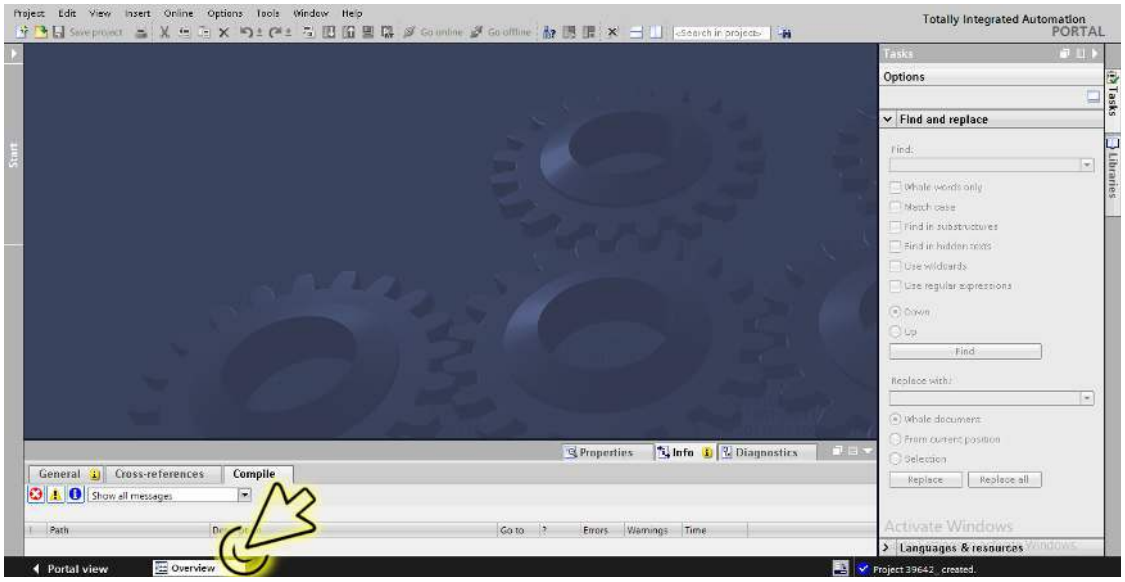
Perform the following steps:

☐ Click the *Project view* icon.



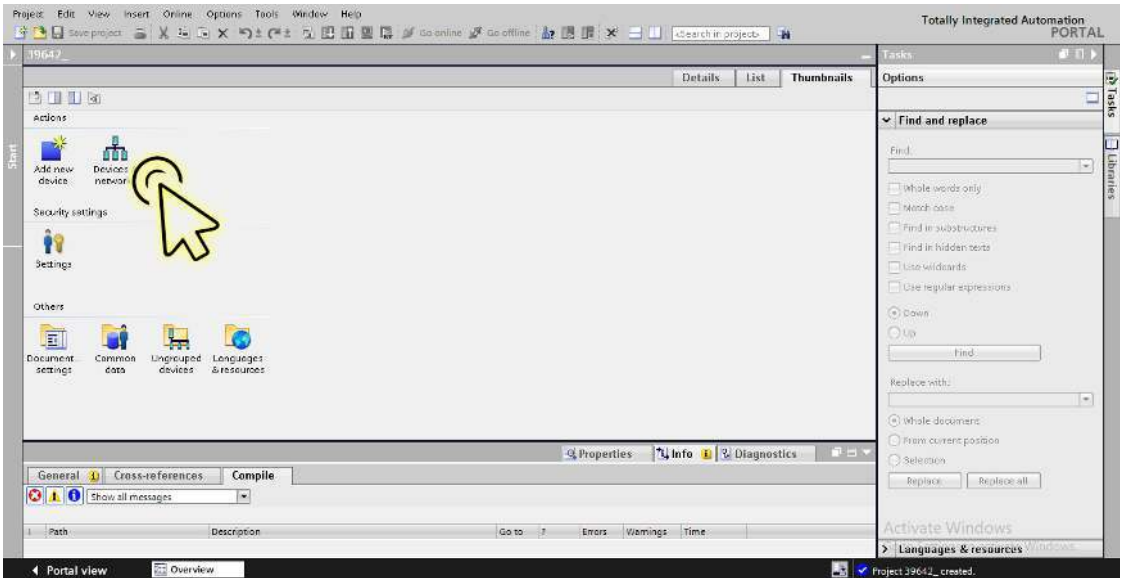
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



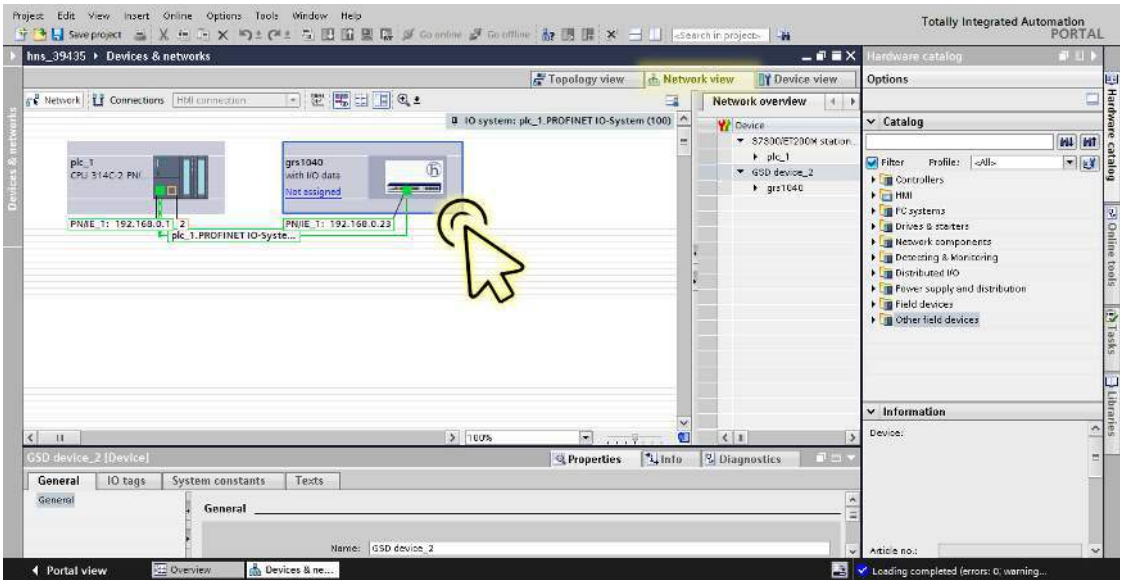
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

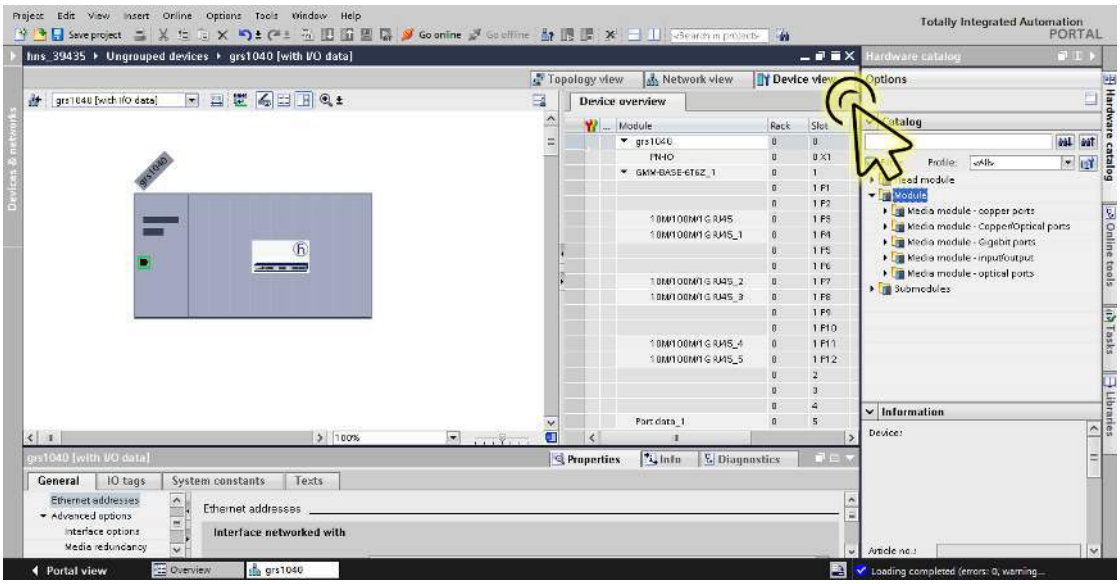


The dialog displays the *Devices & networks* window.

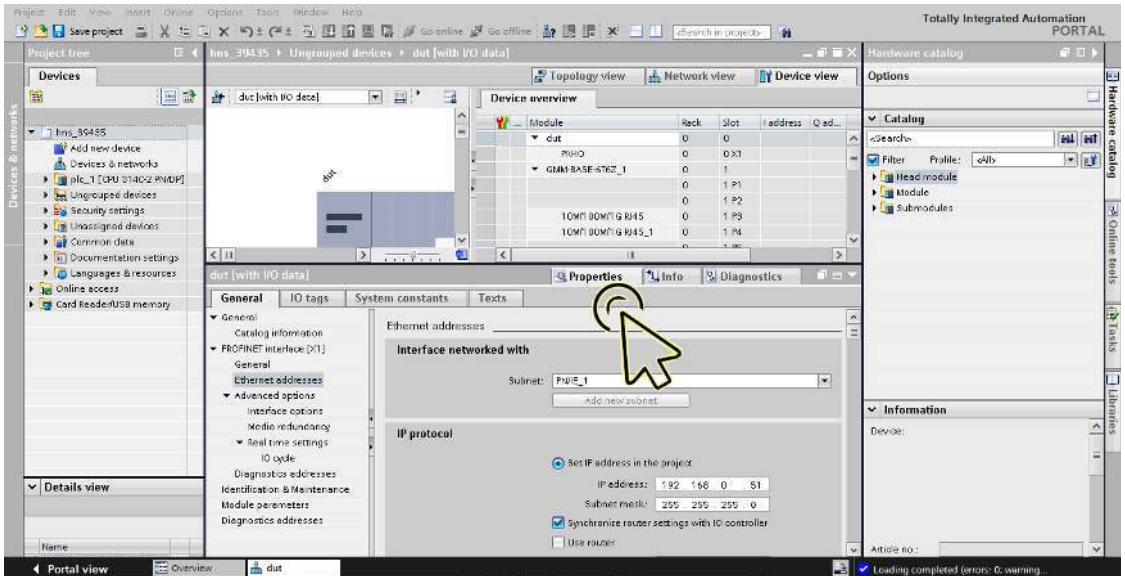
☐ In the *Network view* tab, click the icon of the device.



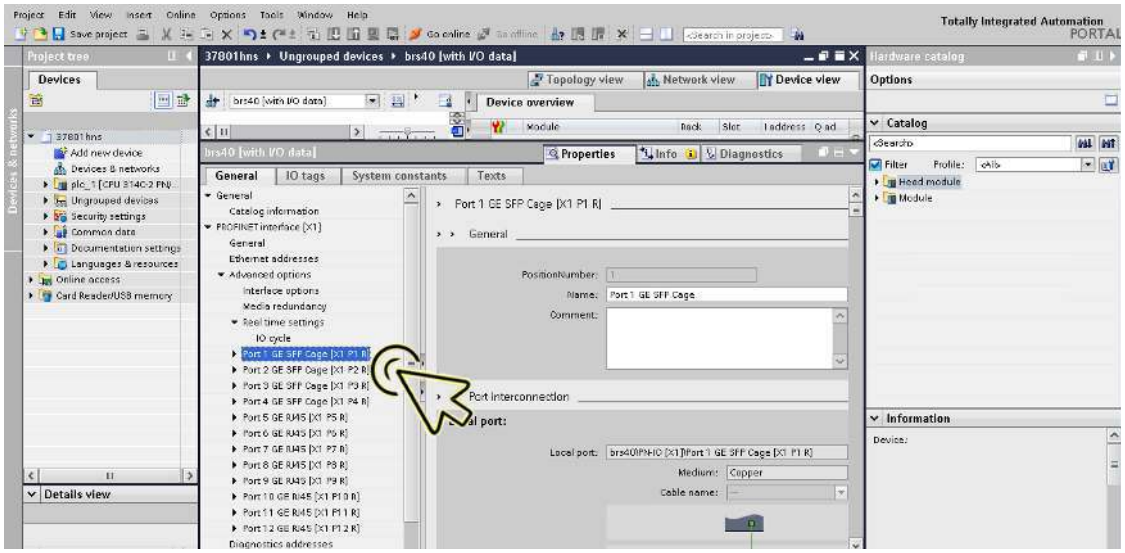
☐ Select the *Device view* tab to display the device details.



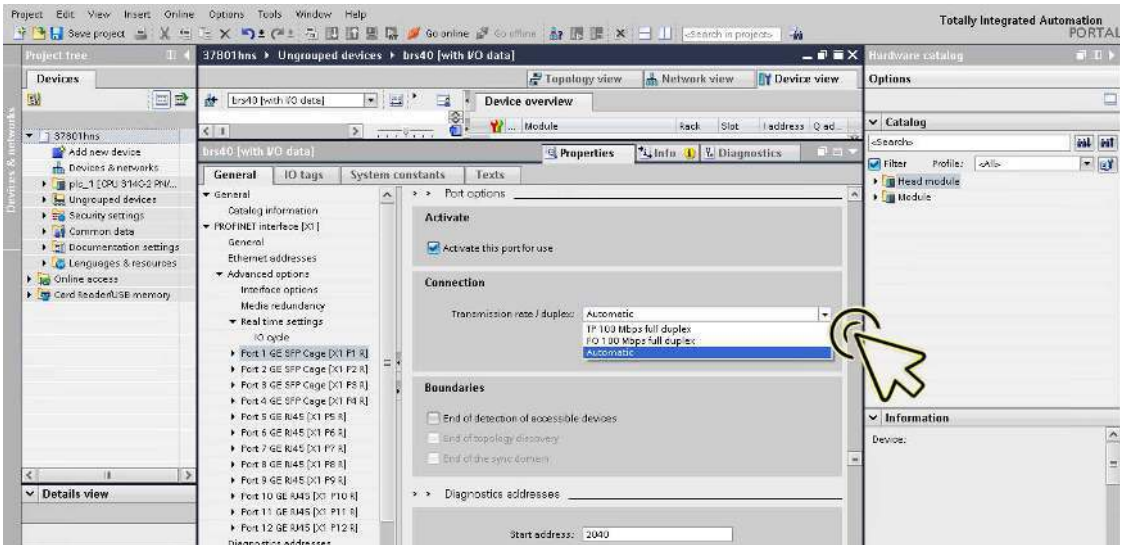
☐ Select the *Properties* tab.
The *Properties* tab contains additional tabs.



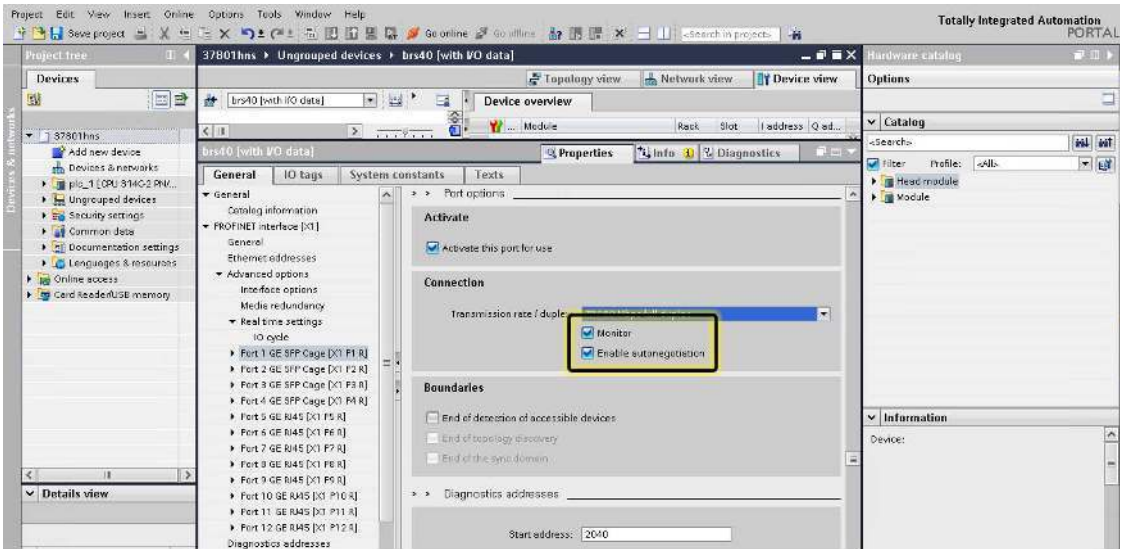
☐ In the *General* tab, navigate to the *PROFINET interface [X1] > Advanced options* item, then click the required port.



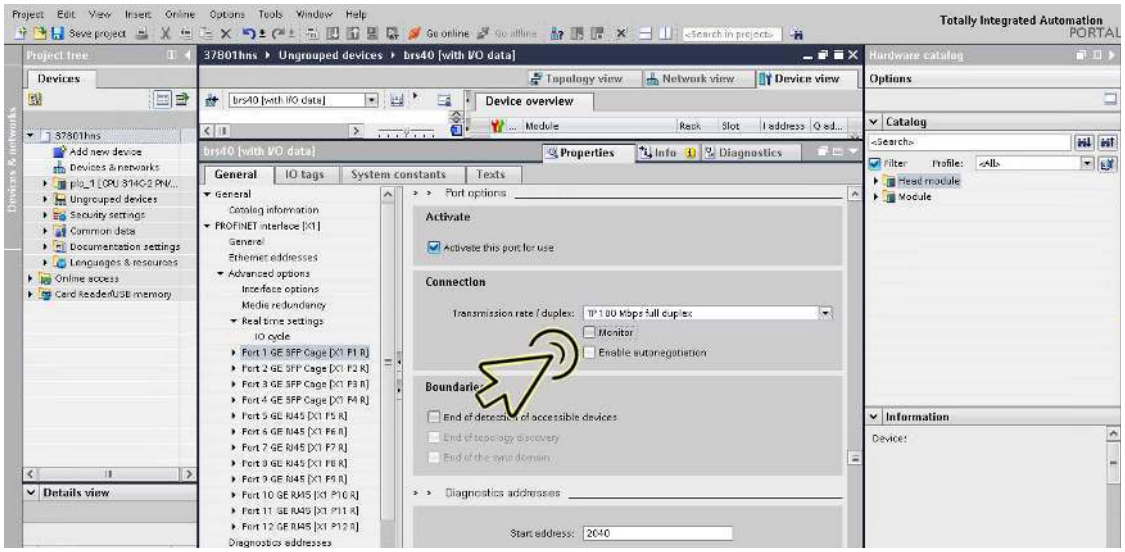
☐ In the *Port options* section, *Connection* frame, select the desired item from the *Transmission rate/ duplex* drop-down list other than the *Automatic* item.



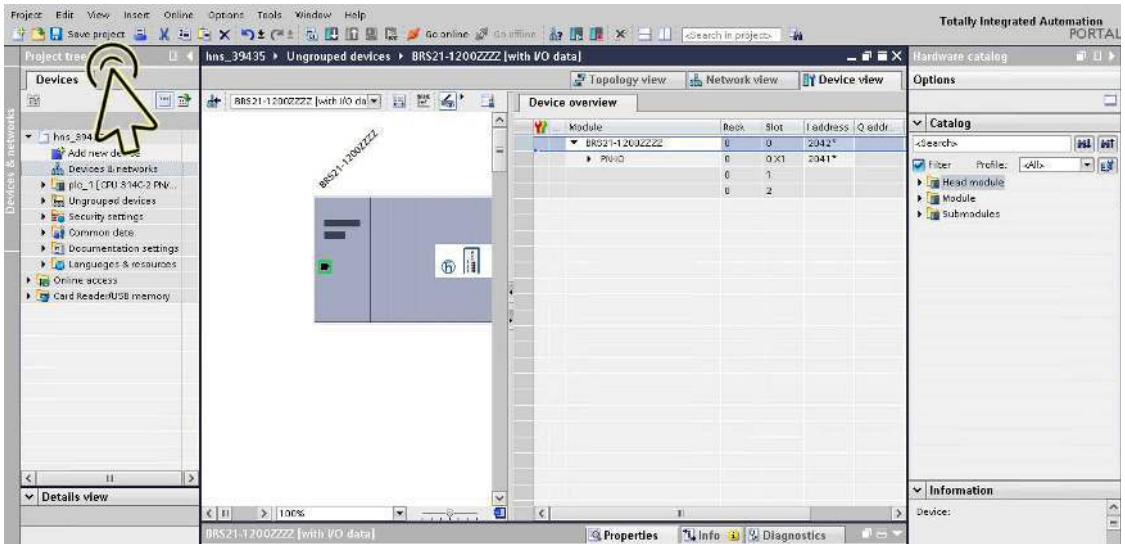
The device automatically marks the *Monitor* and *Enable autonegotiation* checkboxes.



☐ Unmark the *Monitor* and *Enable autonegotiation* checkboxes.



☐ Click the *Save project* button.



If you change the port setting to a value other than `Automatic settings`, then the device disables the port for a short time. If you have positioned the port on the path between the I/O controller and the I/O device, then this interruption can possibly lead to a failure in establishing the Application Relation. Make the following provisions before changing the port setting:

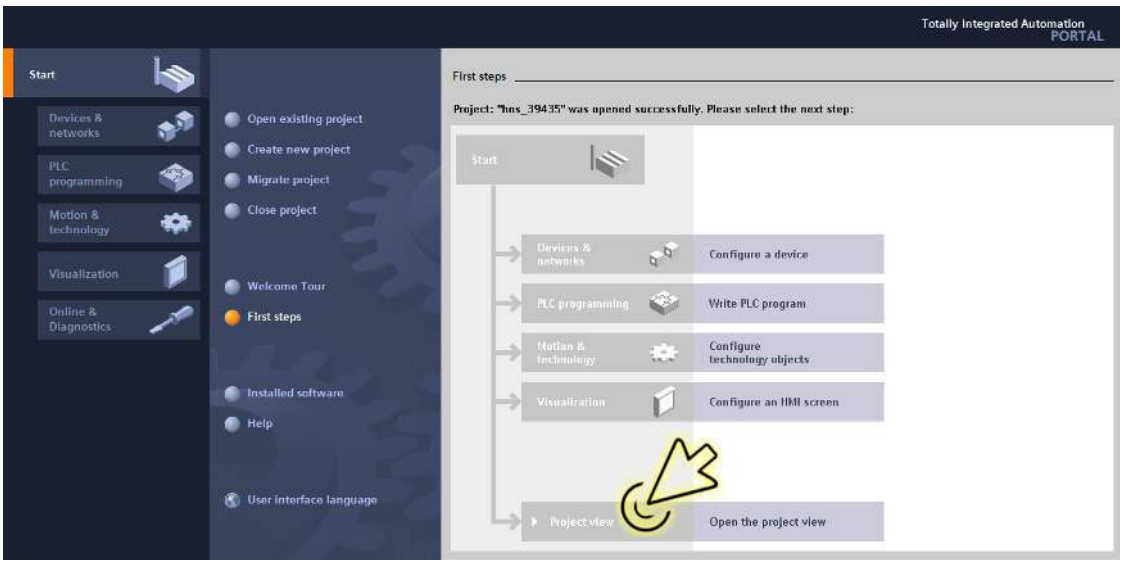
Note:
Before disabling RSTP on certain ports, make sure that this will not result in loops.

Deactivate RSTP on the ports between the I/O controller and the I/O device.

☐ Open the *Switching > L2-Redundancy > Spanning Tree > Port* dialog, *CIST* tab.
☐ Unmark the *STP active* checkbox for the relevant ports.
☐ Apply the settings temporarily. To do this, click the ✓ button.

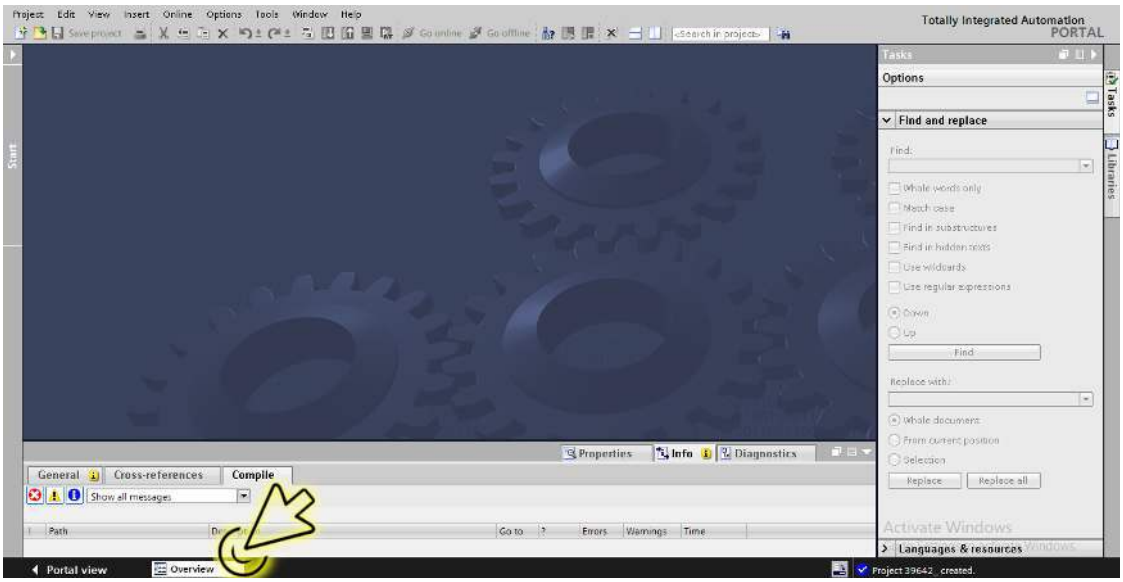
Set up the topology monitoring alarm. To do this, perform the following steps:

☐ Click the *Project view* icon.



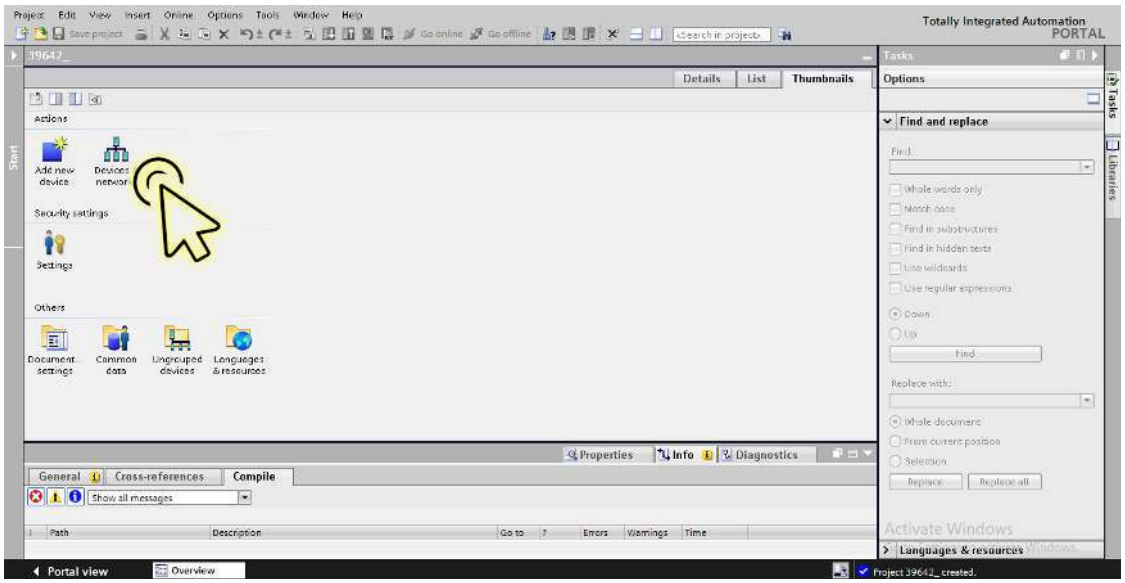
The dialog displays the *Project view* window.

☐ Click the *Overview* tab in the footer.



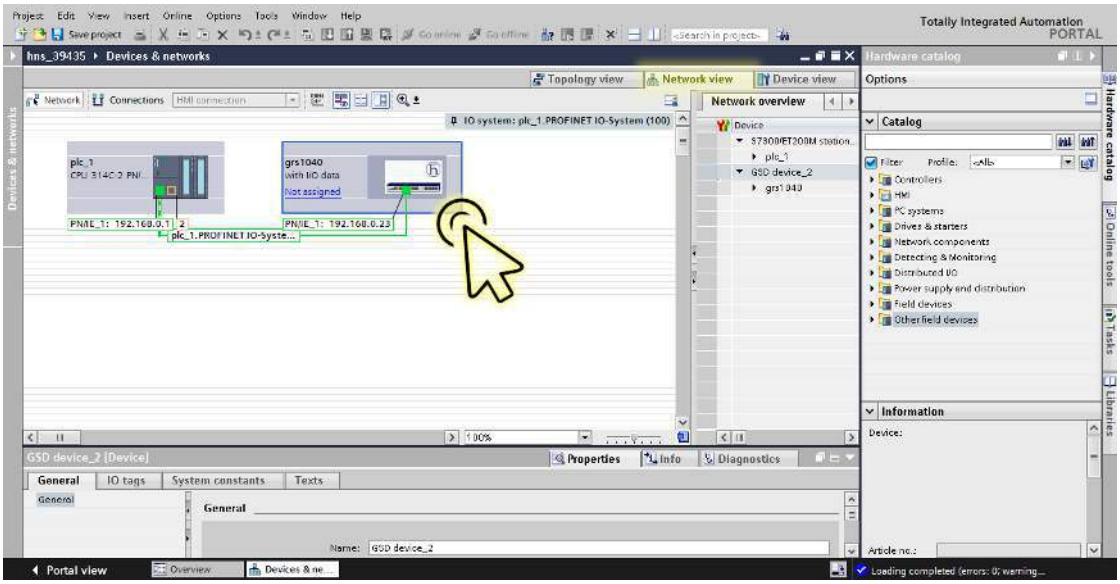
The dialog displays the *Overview* window.

☐ Double-click the *Devices & networks* icon.

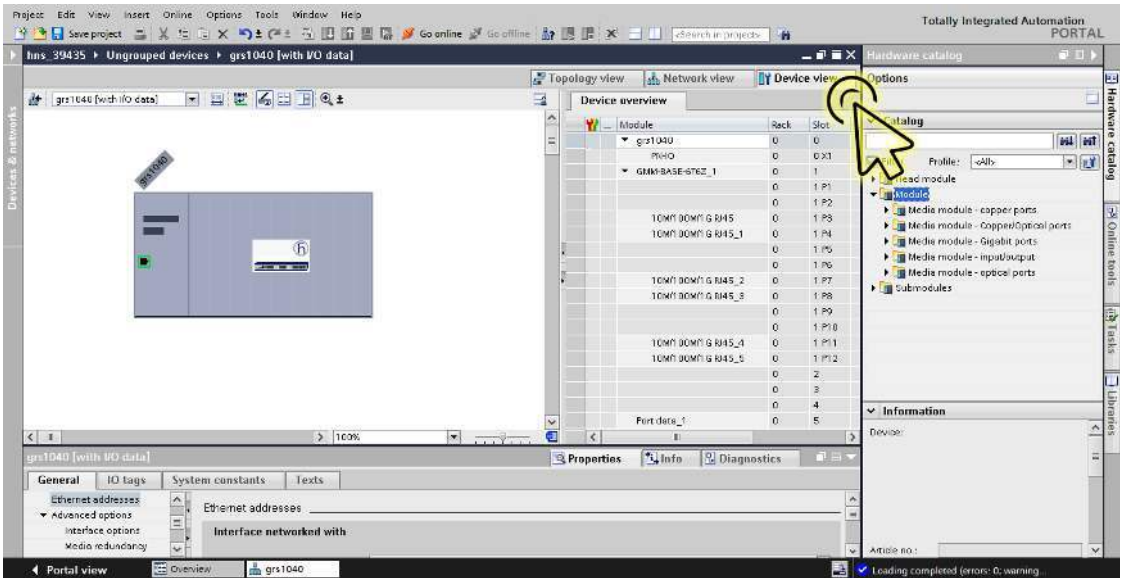


The dialog displays the *Devices & networks* window.

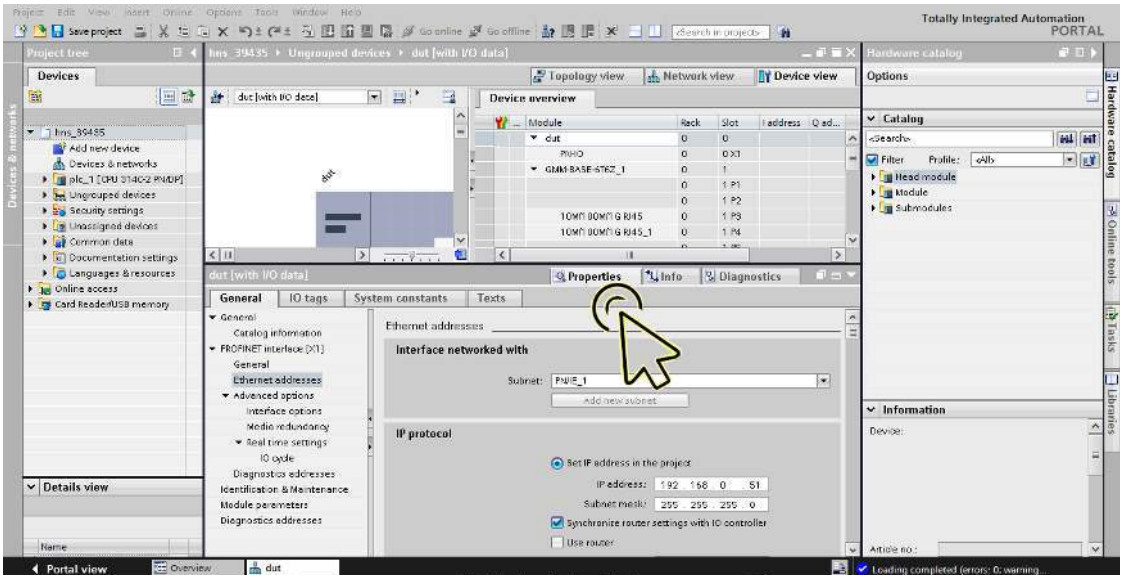
☐ In the *Network view* tab, click the icon of the device.



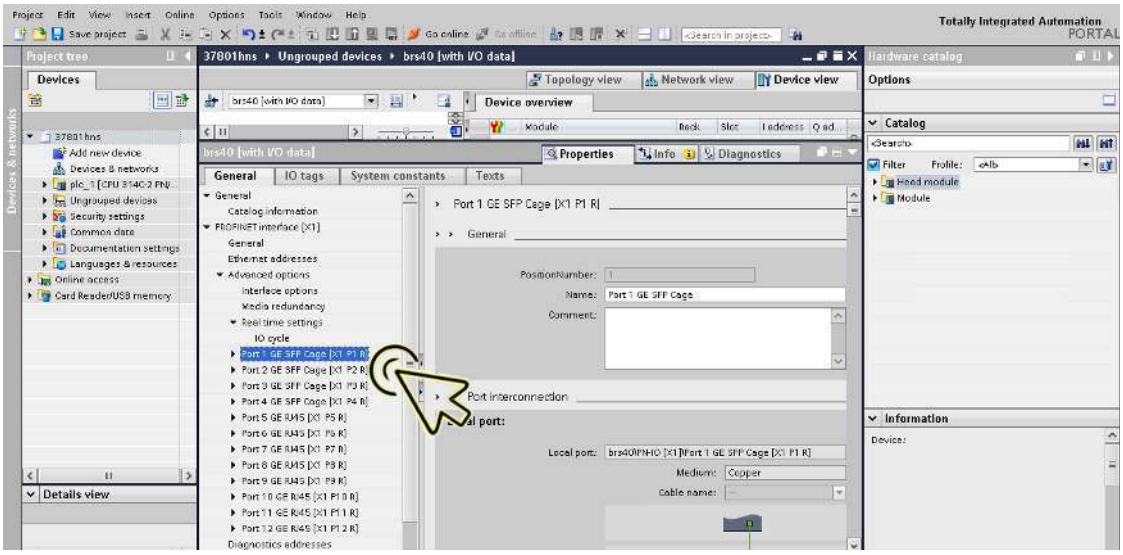
☐ Select the *Device view* tab to display the device details.



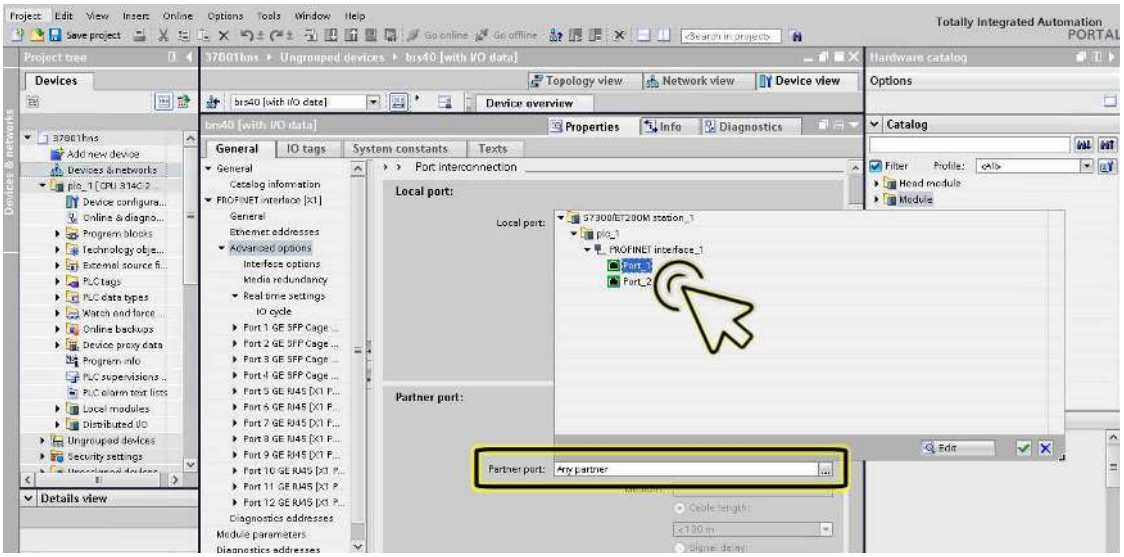
☐ Select the *Properties* tab.
The *Properties* tab contains additional tabs.



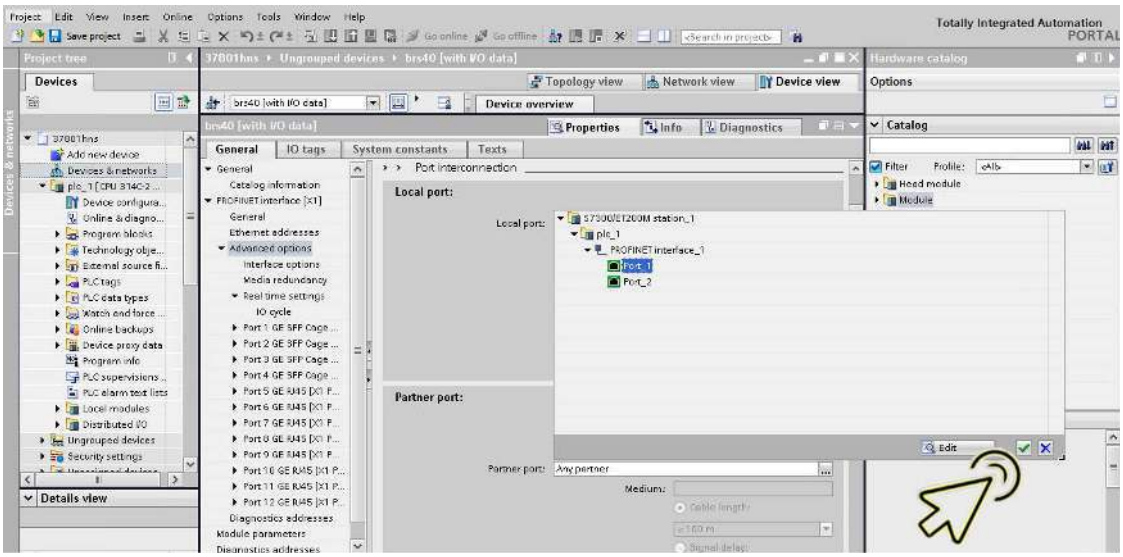
☐ In the *General* tab, navigate to the *PROFINET interface [X1] > Advanced options* item, then click the required port.



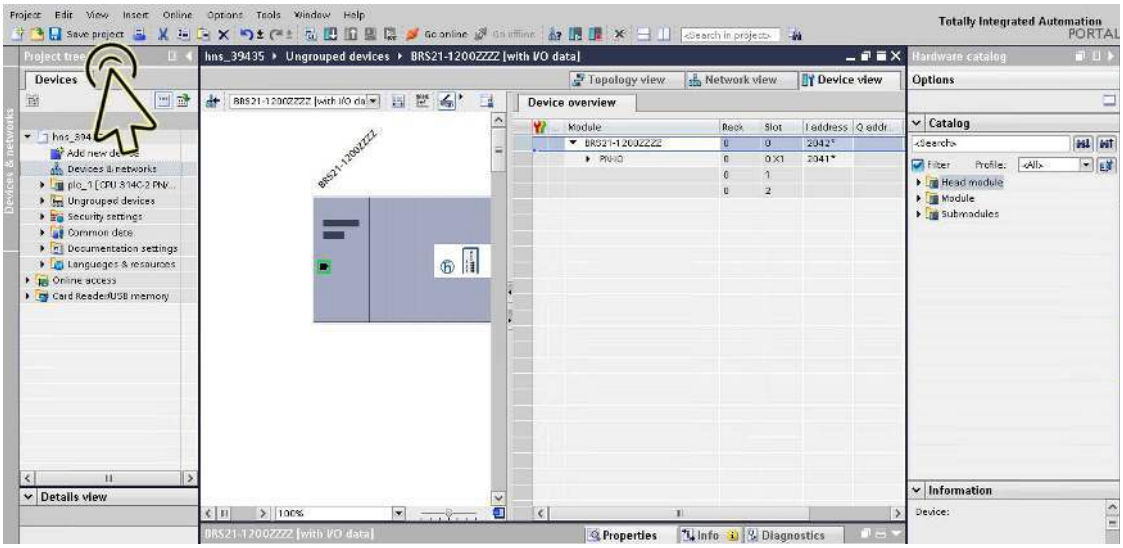
- In the *Port interconnection* section, *Partner port* frame, *Partner port* field, browse and select the port of the partner device with which the device is connected.



☐ To apply the changes, click the ✓ button.



☐ Click the *Save project* button.



Note:
PROFINET monitors the topology configuration. If you connect the port of the Hirschmann device to a different port of the partner device, then the Hirschmann device generates an alarm with the error message `Wrong partner port`.
The alarm ceases when you reconnect the port of the Hirschmann device to the set-up port of the partner device.

Swapping devices

Hirschmann devices support the device swapping function with an engineering station.

When identical devices are swapped, the engineering station assigns the parameters of the original device to the new device.

The device swapping function with the TIA Portal has the following prerequisites:
- S7 1511 with software release from v2.6, currently available for CPU 1511 or higher
- Hirschmann device software release from 08.8.00

- The neighboring devices support *LLDP*.
- The topology is set up and loaded onto the TIA Portal.

Prerequisites for the replacement device:
- The replacement device is exactly of the same type as the original device.
- The replacement device is connected to the exact same place in the network (same ports and neighboring devices).
- The replacement device has a *PROFINET* default configuration:
  - System name = "" (empty string)
  - IP address = 0.0.0.0
    Netmask = 0.0.0.0
    Gateway address = 0.0.0.0
    or
    DHCP is activated
  - *PROFINET* is activated

When these conditions are met, the engineering station automatically assigns the parameters of the original device (device name, IP parameters, and configuration data) to the replacement device.

Perform the following steps:
☐ Make a note of the port assignments on the original device. Remove the original device from the system.
The PLC now detects an error.
☐ Insert the replacement device in the same position in the network. When you reconnect the ports, verify that the port assignments are the same as for the original device.
The PLC finds the replacement device and sets it up the same way as the original device.
The PLC then detects proper operation.
☐ When necessary, reset the PLC to `Run`.

Topology discovery

After you initialize the Topology discovery, the engineering station looks for connected devices.

Configuring the topology

The TIA Portal gives you the option to set up the topology and monitor it accordingly. The TIA Portal displays the connection parameters (quality and settings) in a colored graphic.

Communication diagnosis

The TIA Portal monitors the communication quality and outputs messages relating to detected communication problems.

16.4.5 Activating the Preserve VLAN-0 tag function

The device uses the *Preserve VLAN-0 tag* function to preserve the VLAN tags in received packets that contain a VLAN tag with a VLAN ID of `0`. These packets are also called priority tagged packets. The prerequisite is that the *PROFINET* function is active.

In the default setting, the *Preserve VLAN-0 tag* function is disabled. The device removes the VLAN tag from received packets that contain a VLAN tag with a VLAN ID of `0 during outgoing transmission`.

To activate the *Preserve VLAN-0 tag* function, perform the following steps:

- ☐ Open the *Advanced > Industrial Protocols > PROFINET* dialog.
- ☐ Enable the *PROFINET* function.
  Select the *On* radio button in the *Operation* frame.
- ☐ Activate the *Preserve VLAN-0 tag* function. To do this, mark the *Preserve VLAN-0 tag* 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.
`profinet operation`	To enable the *PROFINET* function.
`profinet vlan-0 forwarding enable`	To activate the *Preserve VLAN-0 tag* function.

16.4.6 PROFINET parameters

Alarms

The device supports alarms on the device and port levels.

Table 65: Alarms supported

Alarms on device level	Change in device status
	Failure of redundant power supply
	Failure/removal of ACA
	Removal of modules
Alarms on port level	Change in link status

Record parameters

The device provides records for:
- Device parameters
- Device status
- Port status/parameters

Table 66: Device parameters

Byte	Content	Access	Value	Meaning
0	Send alarm if status changes	rw	0	Do not send an alarm
			1	Send an alarm if the status of device changes.
1	Power Alarm	rw	0	Do not send an alarm
			1	When a power supply fails, send an alarm.
2	ACA Alarm	rw	0	Do not send an alarm
			1	When the ACA is removed, send an alarm.
3	Module Alarm	rw	0	Do not send an alarm
			1	When the module connections are changed, send an alarm.

Table 67: Device status

Byte	Content	Access	Value	Meaning
0	Device status	ro	0	Unavailable
			1	OK
			2	Error
1	Power supply unit 1	ro	0	Unavailable
			1	OK
			2	Error
2	Power supply unit 2	ro	0	OK
			1	Unavailable
			2	Error
3	Power supply unit 3	ro	0	Unavailable
			1	OK
			2	Error
4	Power supply unit 4	ro	0	Unavailable
			1	OK
			2	Error
5	Power supply unit 5	ro	0	Unavailable
			1	OK
			2	Error
6	Power supply unit 6	ro	0	Unavailable
			1	OK
			2	Error
7	Power supply unit 7	ro	0	Unavailable
			1	OK
			2	Error

Table 67: Device status

Byte	Content	Access	Value	Meaning
8	Power supply unit 8	ro	0	Unavailable
			1	OK
			2	Error
9	Signal contact 1	ro	0	Unavailable
			1	Closed
			2	Open
10	Signal contact 2	ro	0	Unavailable
			1	Closed
			2	Open
11	Temperature	ro	0	Unavailable
			1	OK
			2	Threshold value for temperature exceeded or not reached
12	Fan	ro	0	Unavailable
			1	OK
			2	Fan failure
13	Module removal	ro	0	Unavailable
			1	OK
			2	A module has been removed.
14	ACA removed	ro	0	Unavailable
			1	OK
			2	The ACA has been removed.
15	Not used		0	
			1	
			2	
16	Not used		0	
			1	
			2	
17	Connection	ro	0	Unavailable
			1	OK
			2	Connection failure

Table 68: Port status/parameters

Byte	Content	Access	Value	Meaning
0	Report port error	rw	0	Do not send an alarm
			1	When one of the port alarm reasons represented by bytes 4 .. 10 occurs, send an alarm.
1	Report connection error	rw	0	Do not send an alarm
			1	Send alarm if the connection has failed.

Table 68: Port status/parameters

Byte	Content	Access	Value	Meaning
2	Transmission rate too high **Note:** The configuration of this parameter might not be available in the TIA Portal.	rw	0	Do not send an alarm
			1	When the threshold values for the transmission rate are exceed, send an alarm.
3	Port on	rw	0	Unavailable
			1	Port enabled
			2	Port disabled
4	Link status	ro	0	Unavailable
			1	Connection exists
			2	Connection interrupted
5	Bit rate	ro	0	Unavailable
			1	Unknown
			2	10 Mbit/s
			3	100 Mbit/s
			4	1 Gbit/s
6	Duplex	ro	0	Unavailable
			1	Half-duplex
			2	Full-duplex
7	Auto-negotiation	ro	0	Unavailable
			1	Disabled
			2	Enabled

I/O Data

You find the bit assignment for the I/O data in the following table.

Table 69: Device I/O data

Direction	Byte	Bit	Meaning
	Bit values:	0	OK or unavailable
		1	Reason for report exists
Input	0	General	
		0	Device status
		1	Signal contact 1
		2	Signal contact 2
		3	Temperature
		4	Fan
		5	Module removal
		6	ACA removed
		7	Not used

Table 69: Device I/O data

Direction	Byte	Bit	Meaning
Input	1	Power supply status	
		0	Power supply unit 1
		1	Power supply unit 2
		2	Power supply unit 3
		3	Power supply unit 4
		4	Power supply unit 5
		5	Power supply unit 6
		6	Power supply unit 7
		7	Power supply unit 8
Input	2	Supply voltage status	
		0	Not used
		1	Not used
		2	Connection error
		3	Not used
		4	Not used
		5	Not used
		6	Not used
		7	Not used
Output			Not defined

Table 70: Port I/O data (Input)

Direction	Byte	Bit	Meaning
	Bit values:	0	No connection
		1	Active connection
Input	0	Connection status for ports 1 to 8	
		0	Port 1
		1	Port 2
		2	Port 3
		3	Port 4
		4	Port 5
		5	Port 6
		6	Port 7
		7	Port 8
Input	1	Connection status for ports 9 to 16	
		0	Port 9
		1	Port 10
		2	Port 11
		3	Port 12
		4	Port 13
		5	Port 14
		6	Port 15
		7	Port 16

Table 70: Port I/O data (Input)

Direction	Byte	Bit	Meaning
Input	n	Connection for port (n x 8) + 1 to port (n x 8) + 8	
		0	Port (n x 8) + 1
		1	Port (n x 8) + 2
		2	Port (n x 8) + 3
		3	Port (n x 8) + 4
		4	Port (n x 8) + 5
		5	Port (n x 8) + 6
		6	Port (n x 8) + 7
		7	Port (n x 8) + 8

Table 71: Port I/O data (Output)

Direction	Byte	Bit	Meaning
	Bit values:	0	Port activated
		1	Port not activated
Output	0	Status "Port activated" for ports 1 to 8	
		0	Port 1 activated
		1	Port 2 activated
		2	Port 3 activated
		3	Port 4 activated
		4	Port 5 activated
		5	Port 6 activated
		6	Port 7 activated
		7	Port 8 activated
Output	1	Status "Port activated" for ports 9 to 16	
		0	Port 9 activated
		1	Port 10 activated
		2	Port 11 activated
		3	Port 12 activated
		4	Port 13 activated
		5	Port 14 activated
		6	Port 15 activated
		7	Port 16 activated
Output	n	Status "Port activated" for port (n x 8) + 1 to port (n x 8) + 8	
		0	Port (n x 8) + 1 activated
		1	Port (n x 8) + 2 activated
		2	Port (n x 8) + 3 activated
		3	Port (n x 8) + 4 activated
		4	Port (n x 8) + 5 activated
		5	Port (n x 8) + 6 activated
		6	Port (n x 8) + 7 activated
		7	Port (n x 8) + 8 activated

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.

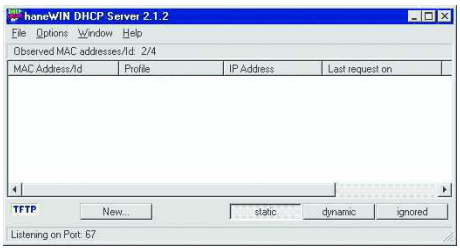


Figure 55: Start window of the haneWIN DHCP Server program

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 56: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.

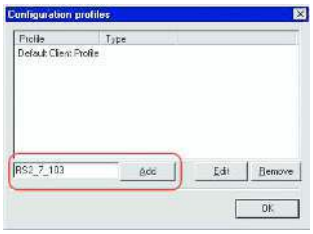


Figure 57:Adding configuration profiles

☐ Click the *Add* button.
☐ Specify the netmask.

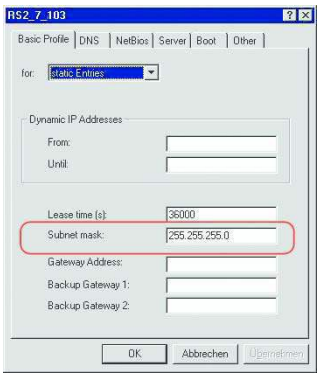


Figure 58:Netmask in the configuration profile

☐ 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.

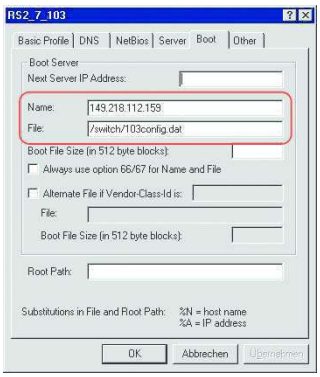


Figure 59:Configuration file on the tftp server

☐ 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.

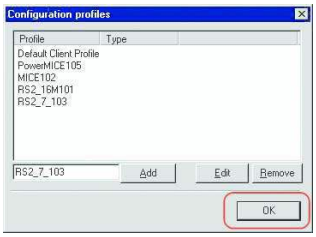


Figure 60:Managing configuration profiles

☐ 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.

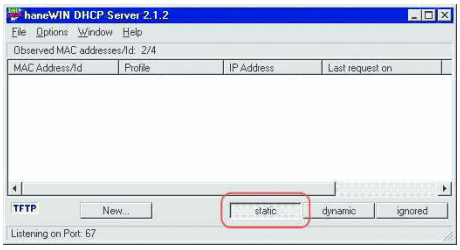


Figure 61:Static address input

☐ Click the *Add* button.

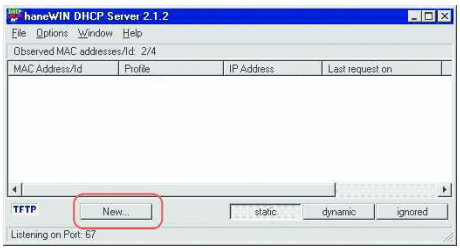


Figure 62:Adding static addresses

☐ Enter the MAC address of the device.
☐ Enter the IP address of the device.

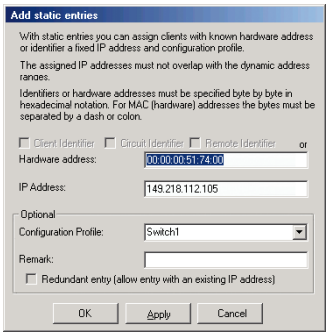


Figure 63:Entries for static addresses

☐ 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.

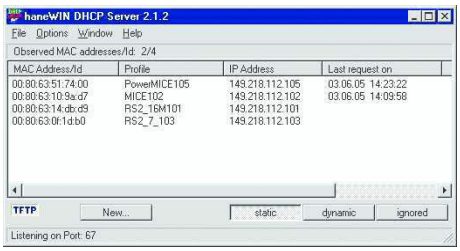


Figure 64:DHCP server with entries

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.

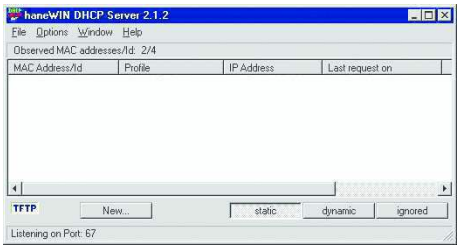


Figure 65: Start window of the haneWIN DHCP Server program

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.

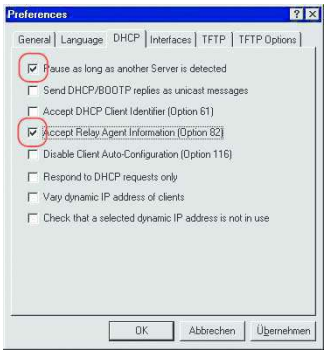


Figure 66: DHCP setting

- ☐ To enter the static addresses, click the *Add* button.

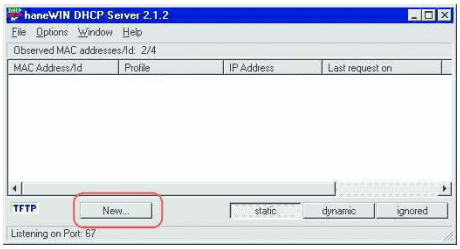


Figure 67: Adding static addresses

- ☐ Mark the *Circuit Identifier* checkbox.
- ☐ Mark the *Remote Identifier* checkbox.

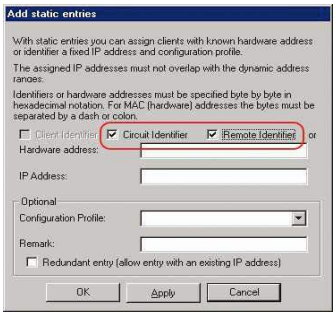


Figure 68: Default setting for the fixed address assignment

- ☐ 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 69: Specifying the addresses

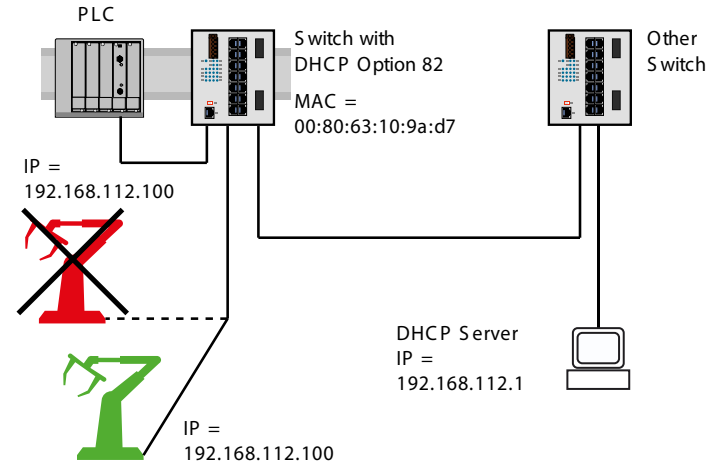


Figure 70: Application example of using Option 82

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`.

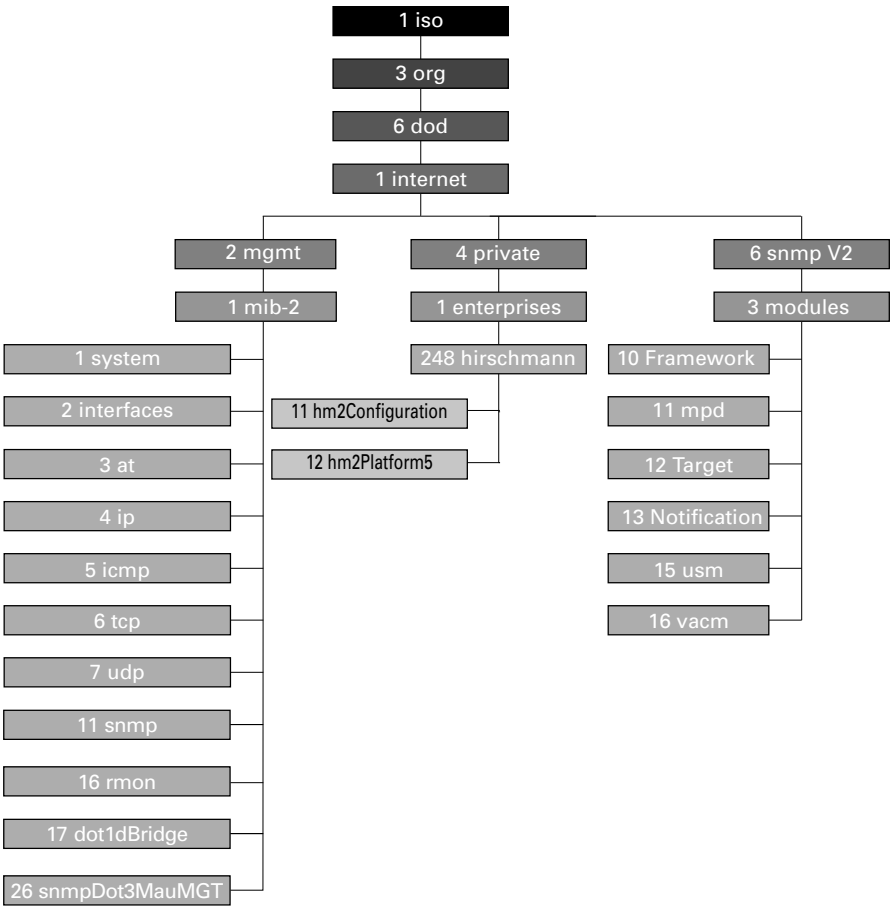


Figure 71: Tree structure of the Hirschmann MIB

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 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 3621	Power Ethernet MIB
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 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)	16384
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)	64
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)	9720 Bytes

B.7.2 VLAN

VLAN ID range	1..4042
Number of VLANs	max. 128 simultaneously per device max. 128 simultaneously per port

B.7.3 Access Control Lists (ACL)

Max. number of ACLs	50
Max. number of rules per ACL	256
Max. number of rules per port	256
Number of total configurable rules	2048 (8 × 256)
Max. number of VLAN assignments	12
Max. number of rules which log an event	128
Max. number of Ingress rules	514

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
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
802.1X 68

A
Access roles 71
Access security 125
Advanced Information, HIPER Ring 210
Advanced Information, MRP 204
Advanced mode 203, 206
Aging time 161
Alarm 236, 367
Alarm messages 235
Alarm setting 312
Alternate port 221, 227
APNIC 46
ARIN 46
ARP 48
Authentication list 68
Automatic configuration 126

B
Backup port 222, 227
Bandwidth 178
Best Master Clock algorithm 94, 96
BOOTP 45
Boundary clock (PTP) 93
BPDU 216
BPDU guard 226, 227
Bridge Identifier 213
Bridge Protocol Data Unit 216

C
CIDR 48
CIP 292
Classless inter domain routing 48
Command Line Interface 19
Command tree 27
Common Industrial Protocol 292
Configuration file 62
Configuration modifications 235
Conformity class 310

D
Data stream monitoring Port Mirroring . . . 258
Data traffic . . . 143
Delay (PTP) . . . 94
Delay measurement (PTP) . . . 94
Delay time (MRP) . . . 203
Denial of Service . . . 143
Designated bridge . . . 221
Designated port . . . 221, 226
Destination table . . . 235
Device description language . . . 310
Device replacement . . . 15
Device status . . . 237
DHCP . . . 45
DHCP L2 Relay . . . 268
DHCP server . . . 86, 90, 263, 373, 376
DHCPv6 . . . 63
Diameter (Spanning Tree) . . . 215
DiffServ . . . 167
Disabled port . . . 222
DoS . . . 143
DSCP . . . 167, 176

E
Edge port . . . 221, 226
EDS . . . 292
Engineering Station . . . 365
Engineering system . . . 312
EtherNet/IP website . . . 292
Event log . . . 254

F
FDB (MAC address table) . . . 157
First installation . . . 45
Flow control . . . 178

G
GARP . . . 272
Gateway . . . 46, 55
Generic Ethernet Module . . . 293
Generic object classes . . . 384
Global Config mode . . . 25
GMRP . . . 272
Grandmaster (PTP) . . . 94, 96
GSD . . . 310, 312, 316
GSD file . . . 316
GSDML . . . 310

H
HaneWin . . . 373, 376
Hardware reset . . . 235
HiDiscovery . . . 45
HIPER Ring . . . 209
HIPER Ring Advanced Information . . . 210
HIPER Ring Packet Prioritization . . . 211
HIPER Ring Packets . . . 210
HiView . . . 67
Host address . . . 46

I
IANA . . . 46
IAS . . . 68
Icon . . . 312
IEC 61850 . . . 280
IEEE MAC address . . . 248
IEEE 802.1X . . . 68
IGMP snooping . . . 161, 292
Industrial HiVision . . . 13
Instantiation . . . 384
Integrated Authentication Server . . . 68
IP address . . . 46, 55, 62
IP header . . . 167, 169
IPv6 address . . . 50
IPv6 address types . . . 51
ISO/OSI layer model . . . 48

L
LACNIC . . . 46
Leave message . . . 161
Link Aggregation . . . 200
Link monitoring . . . 237
Login dialog . . . 18
Loop guard . . . 227, 229

M
MAC address filter . . . 157
MAC destination address . . . 48
MAC address table (forwarding database) . . . 157
MaxAge . . . 216
Memory (RAM) . . . 101
Message . . . 235
MMS . . . 280
Mode . . . 126
MRP . . . 200, 202, 203
MRP Advanced Information . . . 204
MRP Packet Prioritization . . . 205
MRP Packets . . . 204
MRP-IEEE . . . 274
MRP-IEEE operation . . . 274
MRP-IEEE timers . . . 274
Multicast . . . 161

N
Netmask . . . 46, 55
Network load . . . 212, 213
Network management . . . 63
Network structure . . . 202
Non-volatile memory (NVM) . . . 101
NVM (non-volatile memory) . . . 101

O

Object classes . . . 384
Object description . . . 384
Object ID . . . 384
ODVA . . . 292
ODVA website . . . 292
OpenSSH . . . 21, 137
Option 82 . . . 376
Ordinary clock (PTP) . . . 94

P

Path costs . . . 214, 217
PC Worx . . . 312
Polling . . . 235
Port Identifier . . . 213
Port Mirroring . . . 258
Port priority . . . 175
Port roles (RSTP) . . . 221
Port State . . . 222
Prefix length . . . 51
Priority . . . 169
Priority queue . . . 170
Priority tagged frames . . . 169
Privileged Exec mode . . . 24
PROFIBUS Organization . . . 310
Protection functions (guards) . . . 226
PTP . . . 85
PTP domain . . . 95
PuTTY . . . 19, 21

Q

QoS . . . 168
Query . . . 161

R

RADIUS . . . 68
RAM (memory) . . . 101
Rapid Spanning Tree . . . 200, 221
Real time . . . 167
Reconfiguration . . . 213
Reconfiguration time (MRP) . . . 203
Record . . . 368
Redundancy . . . 212
Reference time source . . . 85, 90, 94, 96
Report . . . 251
Report message . . . 161
Request Packet Interval . . . 293
RFC . . . 386
Ring . . . 202
Ring Manager . . . 202
RIPE NCC . . . 46
RM (Ring Manager) . . . 202
RMON probe . . . 258
Root bridge . . . 217
Root guard . . . 226, 229
Root path . . . 218, 219
Root path cost . . . 213
Root port . . . 221, 227
Router . . . 46
Router Advertisement Daemon . . . 60, 64
RPI . . . 293
RST BPDU . . . 221, 223
RSTP . . . 224

S

Secure Shell (SSH) . . . 21
Segmentation . . . 235
Serial connection . . . 19, 39
Service . . . 251
Service Shell . . . 24
Service Shell deactivation . . . 37
Setting the time . . . 85
SNMP . . . 235
SNMP trap . . . 235, 236
SNTP . . . 85
Software version . . . 115
SSH (Secure Shell) . . . 21
Store-and-forward . . . 157
STP-BPDU . . . 216
Strict Priority . . . 170
Subidentifier . . . 384
Subnet . . . 55
Symbol . . . 292, 316
System Monitor 1 . . . 39
System requirements (Graphical User Interface) . . . 17
System time . . . 85

T
Tab Completion 34
TCN guard 227, 229
TCP/IP 292, 310
Technical Documents 403
Technical questions 403
Technical Support 403
Threshold value 312
TIA Portal 312
Topology Change flag 227
ToS 167, 169
Traffic class 170, 175
Traffic shaping 176
Training courses 403
Transmission reliability 235
Transparent clock (PTP) 93
Trap 235, 236
Trap destination table 235
Tree structure (Spanning Tree) 217, 220
TSN 181
Type of Service 169

U
UDP/IP 292, 310
User Exec mode 24
User name 18, 20, 22
Utilization 212, 213

V
Video 170
VLAN 185
VLAN (HIPER Ring) 209
VLAN mode 24
VLAN priority 174
VLAN tag 169, 185
VoIP 170
VT100 terminal emulation 19, 39

W
Weighted Fair Queuing 170
Weighted Round Robin 170

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
BOBCAT IP30/40 Extended Switch
HiOS-2S

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 . . . 24
1.3 Compiling a threat profile . . . 25
1.3.1 Risk value and unit . . . 25
1.3.2 Assess the risk of an individual threat . . . 26
1.4 Defense in depth . . . 27
1.4.1 Introduction . . . 27
1.4.2 Purpose . . . 27
1.4.3 Defense in depth vs. hardening . . . 27
1.4.4 Responsibilities . . . 28
1.4.5 Defense in depth example . . . 28
1.5 Developing a mitigation strategy . . . 30
1.5.1 Assess the efficiency of an individual mitigation measure . . . 30
1.5.2 Mitigation efficiency value and unit . . . 31
1.5.3 Alternatives to mitigation . . . 31
1.6 Criticality assessment and mitigation strategies . . . 33
1.6.1 Mitigation calculation . . . 33
1.6.2 Combining threat risk and mitigation efficiency . . . 33
1.6.3 Recommended mitigation strategies . . . 34
1.6.4 Residual risk . . . 34
1.6.5 Security viewpoints: binary or continuous values . . . 34
1.7 Cryptographic key and password basics . . . 36
1.7.1 Cryptographic key policies . . . 36
1.7.2 Password and cryptographic key comparison . . . 37

1.8 Impact of the system life cycle on the device life cycle . . . 38
1.8.1 VLAN plan . . . 38
1.9 Impact of device requirements on system planning . . . 39
1.9.1 Planning a secure installation location . . . 39
1.9.2 Planning for device availability . . . 40
1.9.3 Planning for Software auto update from the external memory . . . 40
1.9.4 Planning for SSH key auto upload from the External Memory . . . 40
1.9.5 Planning the Configuration load priority for the external memory . . . 40
1.9.6 Planning for device and port LED visibility . . . 41
1.9.7 Planning how to check the security seal . . . 41
1.9.8 Planning restrictions to the device hardware interfaces . . . 41
1.9.9 Planning a secure boot policy <SL-C2> . . . 42
1.9.10 Planning a dedicated user account login policy . . . 42
1.9.11 Planning a dedicated user account password policy . . . 43
1.9.12 Planning a dedicated user account name and access role policy for device management . . . 45
1.9.13 Planning configuration encryption and the associated password . . . 46
1.9.14 Planning session timeouts <SL-C2> . . . 46
1.9.15 Planning a dedicated logging policy . . . 47
1.9.16 Planning a dedicated LLDP policy <SL-C2> . . . 47
1.9.17 VLAN plan considerations depending on redundancy protocols . . . 47
1.9.18 Advanced authentication measures <SL-C2> . . . 48
1.10 Impact of network aspects on system planning . . . 49
1.10.1 External server considerations . . . 49
1.10.2 Software update and configuration server considerations <SL-C2> . . . 49
1.10.3 External DHCP server considerations . . . 50
1.10.4 Network time synchronization considerations <SL-C2> . . . 50
1.10.5 Authentication server considerations <SL-C2> . . . 51
1.10.6 Logging server considerations <SL-C2> . . . 52
1.11 Device-related policies . . . 53
1.11.1 Develop a backup policy for device-related data . . . 53
1.11.2 Develop a policy for replacing the device hardware . . . 53
1.11.3 Develop a policy for device hardware repair . . . 53
1.11.4 Develop a policy for device hardware decommissioning . . . 54
1.11.5 Develop a policy for device hardware disposal . . . 55
1.12 Operation and maintenance policy . . . 56
1.13 Document the planned policies . . . 57

2 Device security in the life cycle phases . . . 59
2.1 Develop the device configuration . . . 59
2.2 Software vs. hardware measures (logical vs. physical) . . . 60
2.3 Security-related vs. general device functions . . . 61
2.4 Prerequisites for installation and setup . . . 62
2.4.1 Possible further prerequisites . . . 62
2.5 Suggested installation step sequence . . . 63
2.5.1 Reasons for the suggested installation step sequence . . . 63
2.5.2 Suggested preparation for installation . . . 63
2.6 Choosing a secure installation location . . . 65
2.6.1 Considering the device availability requirements . . . 65
2.7 Considering the power supply redundancy requirements . . . 66
2.8 Considering the power budget requirements . . . 67
2.9 Considering the data link redundancy requirements . . . 68

2.10 Software update . . . 69
2.10.1 Initial access to the device management . . . 69
2.10.2 Initial password considerations . . . 69
2.10.3 Software update server considerations . . . 70
2.10.4 Secure boot considerations . . . 70
2.10.5 Best practices . . . 71
2.10.6 Detailed documentation . . . 71
2.11 Security setup overview . . . 72
2.11.1 Assign IP address parameters to the device management . . . 74
2.11.2 Disable HiDiscovery access . . . 74
2.11.3 Enable the secure boot mode <SL-C2> . . . 75
2.11.4 Enable configuration encryption <SL-C2> . . . 75
2.11.5 Set up a VLAN dedicated to device management access . . . 76
2.11.6 Disable logical access to unused ports . . . 76
2.11.7 Set up Power over Ethernet (depends on hardware) . . . 76
2.11.8 Disable the automatic device software update from the external memory (ACA) . . . 77
2.11.9 Disable the SSH key auto upload from the external memory . . . 77
2.11.10 Disable the Configuration load priority for the external memory . . . 78
2.11.11 Disable copying a software file into the device that lacks a valid cryptographic signature . . . 78
2.11.12 Disable writing an unencrypted configuration profile to the external memory (ACA) . . . 79
2.11.13 Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2> . 79
2.11.14 Disable insecure management protocols . . . 79
2.11.15 Set up management IP access restrictions . . . 79
2.11.16 Set up a dedicated HTTPS certificate for the device . . . 80
2.11.17 Set up a dedicated SSH host key for the device . . . 81
2.11.18 Set up the SSH Known Hosts fingerprints in the device . . . 82
2.11.19 Set up a dedicated user account login policy . . . 82
2.11.20 Set up a dedicated user account password policy . . . 83
2.11.21 Set up dedicated user account names and access roles for device management <SL-C2> . . . 84
2.11.22 Specify finite session timeouts <SL-C2> . . . 86
2.11.23 Set up time synchronization for the device clock <SL-C2> . . . 86
2.11.24 Set up certificates and possible revocation lists for authentication, logging and eMail servers . . . 87
2.11.25 Set up logging . . . 88
2.11.26 Disable SNMPv1 traps . . . 88
2.11.27 Enable SNMPv3 traps . . . 88
2.11.28 Set up dedicated login banners . . . 89
2.11.29 Advanced: Access to the system monitor through the serial port . . . 89
2.11.30 Advanced: disable access to the CLI service shell . . . 89
2.11.31 Set up advanced user authentication <SL-C2> . . . 90
2.11.32 Create a backup of the device-related data . . . 90
2.12 Possible restrictions to the device’s hardware interfaces . . . 92
2.12.1 Restrict physical access to the USB port . . . 92
2.12.2 Restrict physical access to network ports or SFP slots . . . 93
2.12.3 Restrict physical (visual) access to the device LEDs and port LEDs . . . 93
2.13 Device installation . . . 94
2.13.1 Checking the security seal . . . 94
2.13.2 Data connections . . . 94
2.14 Operation . . . 95

2.15 Maintenance . . . 96
2.15.1 Check the security seal (regularly or triggered by an event) . . . 96
2.15.2 Software update . . . 96
2.15.3 Hardware changes . . . 96
2.15.4 Device hardware replacement . . . 97
2.15.5 Device hardware repair . . . 98
2.16 Device decommissioning . . . 100
2.16.1 Deletion of confidential data and secrets . . . 100
2.16.2 Reset to the delivery state . . . 100
2.16.3 Secure physical destruction of the device and its accessories . . . 101
2.16.4 Secure removal of device-related data from the administration environment . . . 101
2.16.5 Secure disposal of the device hardware . . . 101

3 Network security support . . . 103
3.1 Introduction . . . 103
3.1.1 Prerequisites for setting up network security . . . 103
3.1.2 Deploying defense in depth for your network . . . 104
3.1.3 Harden your network . . . 104
3.2 Measures to help secure the network . . . 105
3.3 Restrict logical access to your network . . . 106
3.3.1 Set up VLANs for traffic segregation . . . 106
3.3.2 Disable GVRP and MVRP . . . 106
3.3.3 Set up the Port Security . . . 106
3.4 Help secure the network protocols used . . . 108
3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 108
3.5 Help secure the redundancy protocols used . . . 109
3.5.1 Set up RSTP guards and helper protocols . . . 109
3.5.2 Set up the MRP (Media Redundancy Protocol) parameters. . . . 110
3.5.3 Set up the HIPER Ring parameters . . . 110
3.6 Set up the attack protection support functions . . . 111
3.6.1 Set up the Denial of Service (DoS) parameters . . . 111
3.6.2 Set up the rate limiter . . . 111
3.6.3 Set up the Management MAC address conflict detection . . . 111
3.7 Set up Access Control Lists (ACLs) . . . 112
3.7.1 Introduction . . . 112
3.7.2 Resolving potential conflicts of aims for an ACL . . . 113
3.7.3 Creating ACLs and associations . . . 113
3.8 Set up the network time synchronization parameters <SL-C2> . . . 116
3.9 Set up the logging parameters . . . 117
3.9.1 Audit trail (created by persistent logging) . . . 117
3.10 Set up the LLDP parameters <SL-C2> . . . 118

A Security seal . . . 121
A.1 Overview . . . 121
A.2 Details . . . 122
A.2.1 Glued front label . . . 122
A.2.2 Potted device . . . 123
A.2.3 Security stickers . . . 123

B Password strength and policy guide . . . 125
B.1 Password classes . . . 125
B.2 Password policies . . . 127

B.3 Password schemes . . . 128
B.4 Password attack strategies . . . 129
B.5 Basic security assumptions . . . 130
B.5.1 Aggressive assumptions about attackers . . . 130
B.5.2 Conservative assumptions about users . . . 130
B.5.3 Conservative assumptions about the attack context . . . 131
B.6 Quantitative password strength . . . 132
B.6.1 High-complexity passwords . . . 132
B.6.2 Low-complexity passwords . . . 134
B.7 Attack resistance time (quantitative) . . . 137
B.7.1 Examples, unmitigated attack rate . . . 138
B.7.2 Attack rate mitigation . . . 138
B.7.3 Examples, mitigated attack rate . . . 139
B.8 Required attack resistance time (quantitative) . . . 140
B.9 Password entropy . . . 141
B.10 Calculating the required password entropy . . . 142
B.11 Password policy lookup tables (quantitative) . . . 144
B.11.1 Password entropy lookup tables . . . 144
B.11.2 Password policy lookup table, low-complexity passwords . . . 145
B.11.3 Password policy lookup table, high-complexity passwords . . . 146

C Considerations for manually entered keys . . . 149
C.1 Quantitative key strength . . . 149
C.1.1 Key entry as ASCII string . . . 150
C.1.2 Key entry as hexadecimal string . . . 151
C.1.3 Conclusion . . . 152
C.1.4 Example of random key value generation (tool use) . . . 154

D Index . . . 155

E Technical support . . . 167

F Readers' Comments . . . 168

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 59 “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 103 “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 121 “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 125 “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 149 “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 59 “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 103 “Network security support”)

It deals with the following life cycle phases of your network device:
- Secure installation (see on page 63 “Suggested installation step sequence”)
- Secure setup (see on page 72 “Security setup overview”)
- Secure operation (see on page 95 “Operation”)
- Secure maintenance (see on page 96 “Maintenance”)
- Secure replacement (see on page 97 “Device hardware replacement”)
- Secure repair (see on page 98 “Device hardware repair”)
- Secure decommissioning (see on page 100 “Device decommissioning”)

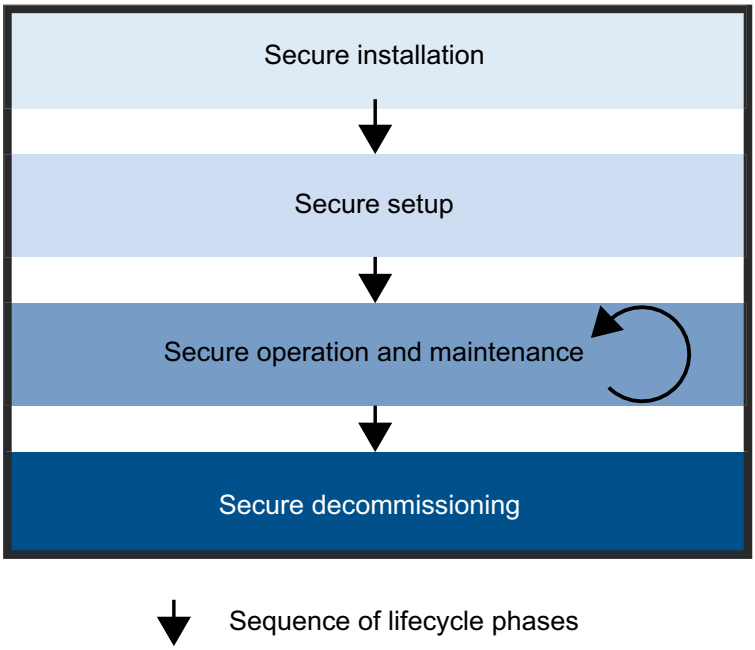


Figure 1: Device life cycle overview

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.

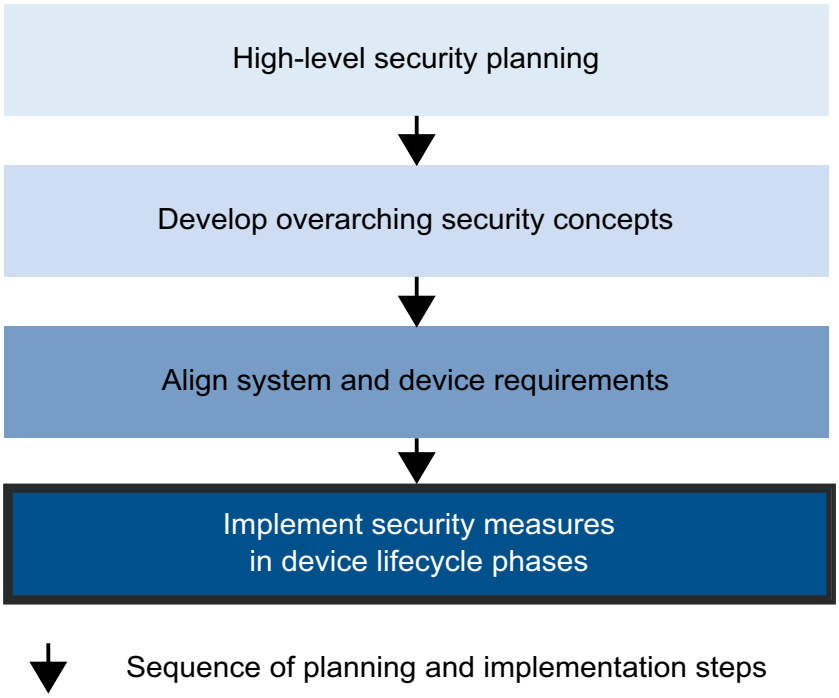


Figure 2: Required preparatory work hierarchy before implementation

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>
- Authentication server considerations <SL-C2>
- 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.

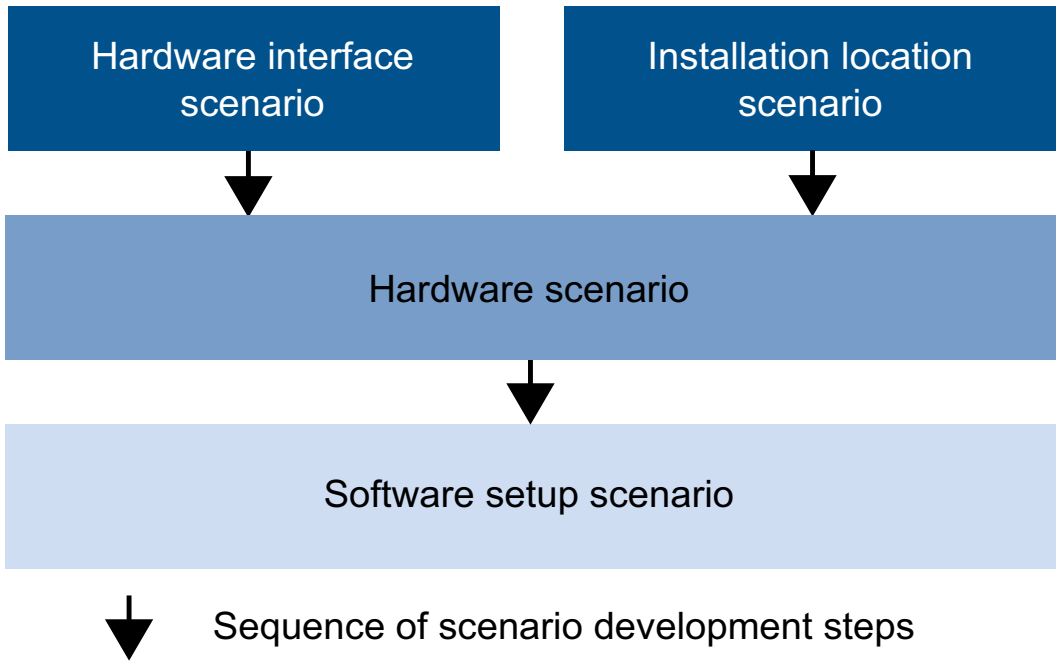


Figure 3: Basic scenario development steps

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.

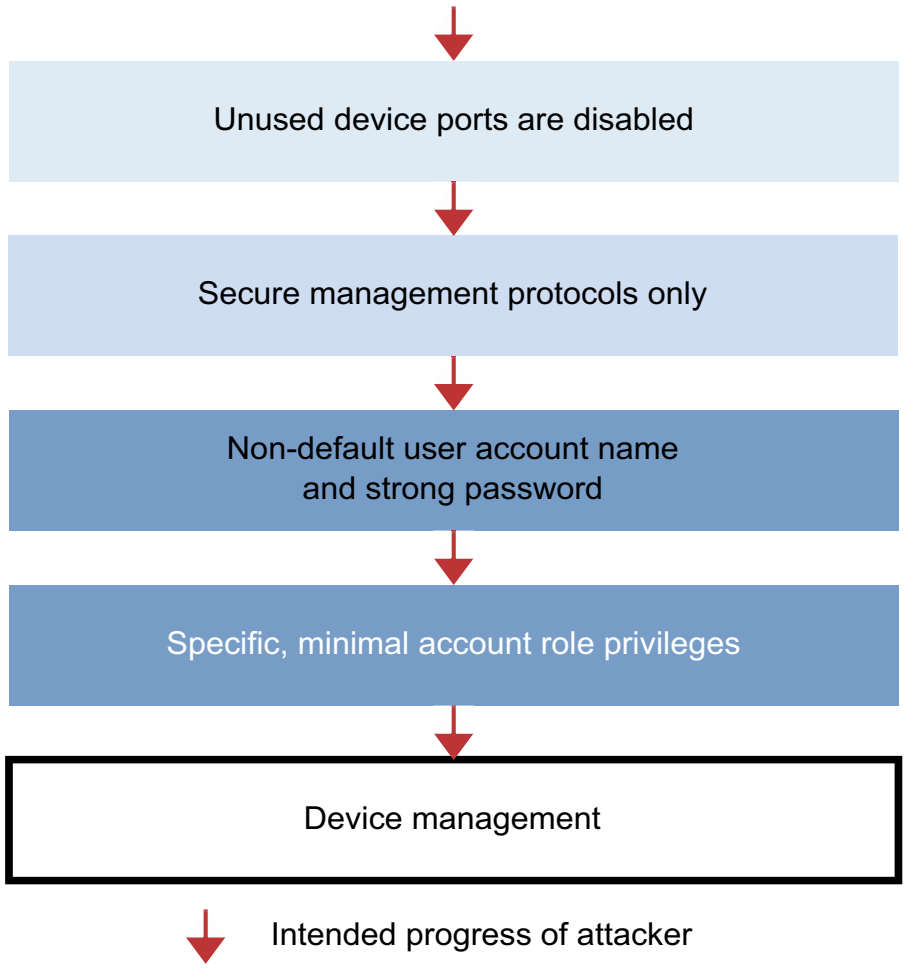


Figure 4: Barrier arrangement example for defense in depth

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 25 “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

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 125 “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 149 “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 47 "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], PoE power budget, and data link redundancy
  - Properties of the USB port
  - 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, a dedicated authentication policy list or RADIUS: 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 dedicated authentication policy list.
  - Plan the RADIUS server setup.

Note:
These topics are covered in more detail in the following main chapter (see on page 65 “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 and for PoE
- 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 77 “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 77 “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 78 “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 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.

1.9.7 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 121 “Security seal”).

1.9.8 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 USB port.
- Restrict physical access to network ports.
- 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.

1.9.9 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 121 “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.

1.9.10 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 138 “Attack rate mitigation”). For quantitative information on how to provide for hard-to-break passwords (see on page 125 “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 125 “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.

1.9.11 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 125 “Password strength and policy guide”).

Consider the type of password you want to use (see on page 132 “Quantitative password strength”):

- High-complexity passwords have the following properties (see on page 132 “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 134 “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 42 “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 82 “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.

1.9.12 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.

1.9.13 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.

1.9.14 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

1.9.15 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 52 “Logging server considerations <SL-C2>”).

Note:
The Syslog (system message logging) client in the device offers unencrypted communication only. 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.

1.9.16 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 118 “Set up the LLDP parameters <SL-C2>”).

1.9.17 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 38 “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

1.9.18 Advanced authentication measures <SL-C2>

If you intend to use advanced user authentication measures like 802.1X or a dedicated authentication policy list:
- Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
- 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 "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
- 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.
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

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 Network time synchronization considerations <SL-C2>

[CR2.11 RE1]

Network time synchronization can be required for several reasons, including secure logging.

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

1.10.5 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 RADIUS 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 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 unobfuscated protocol version of RADIUS implicitly trusts its servers. If you intend to use remote authentication, consider developing an overarching remote authentication policy and using only the obfuscated RADIUS protocol version.

Note:
Encrypted LDAP can be considered preferable over obfuscated RADIUS 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 "Network security > RADIUS" for the device RADIUS client function

1.10.6 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 only.
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.
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

1.11 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 121 “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 121 “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 121 “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 45 “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.
  - 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.

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 72 “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 103 “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 65 “Choosing a secure installation location”)
- ☐ Planning restrictions to the device hardware interfaces (see on page 41 “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 42 “Planning a dedicated user account login policy”)
- ☐ Developing a dedicated user account **password** policy (see on page 43 “Planning a dedicated user account password policy”)
- ☐ Developing a dedicated user account and access role policy for device management (see on page 45 “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 46 “Planning configuration encryption and the associated password”)
- ☐ Planning session timeouts <SL-C2> (see on page 46 “Planning session timeouts <SL-C2>”)
- ☐ Developing a dedicated logging policy, possibly including remote logging (see on page 47 “Planning a dedicated logging policy”)
- ☐ Developing a policy for the servers that hold device software updates and configuration files <SL-C2> (see on page 49 “Software update and configuration server considerations <SL-C2>”)
- ☐ Planning a dedicated LLDP policy <SL-C2> (see on page 47 “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>
- ☐ Authentication server considerations <SL-C2>
- ☐ 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 65 “Choosing a secure installation location”)
- ☐ Perform the initial software update (see on page 69 “Software update”)
- ☐ Perform the initial security setup (see on page 72 “Security setup overview”)
- ☐ If required, modify the hardware interfaces for security (see on page 92 “Possible restrictions to the device’s hardware interfaces”)
- ☐ Perform the initial device installation (see on page 94 “Device installation”)
- ☐ Operation measures (see on page 95 “Operation”)
- ☐ Maintenance measures (see on page 96 “Maintenance”)
- ☐ Decommissioning measures (see on page 100 “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, 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 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 121 “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 75 “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 39 “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 93 “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 66 “Considering the power supply redundancy requirements”).
- Consider the power budget requirements (see on page 67 “Considering the power budget requirements”).
- Consider the data link redundancy requirements (see on page 68 “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.
- One single power supply can also deliver the worst-case set-up PoE or PoE+ power. **(depends on hardware)**

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 43 “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 82 “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 42 “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 46 “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 53 “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 69 “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 43 “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 82 “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 92 “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.
- Set up Power over Ethernet. **(depends on hardware)**
- 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.

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 90 “Set up advanced user authentication <SL-C2>”):
- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - RADIUS

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 43 “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 42 “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 42 “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 46 “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 36 “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 47 “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 unused ports

In the delivery state, every port is enabled ⚠.

Disable network access for unused ports. 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.

2.11.7 Set up Power over Ethernet (depends on hardware)

Delivery state:
- The device-global setting `PoE Global Operation` is *`On`*.
- Port-related settings:
  - The setting `PoE Port Enable` is *`PoE enable`*.
  - The allowed classes, *`Class 0`*..*`Class 4`*, are enabled.
  - The `Power limit [W]` is `0.0` — the device will not enforce a specific power limit.
  - The power PoE `Priority` is *`low`*.

Device security aspects:
- If you do not need PoE or PoE+, disable PoE and PoE+ globally in the device.
- If you need PoE or PoE+:
  - Disable PoE or PoE+ on those ports that shall not deliver power.
  - For each port with PoE or PoE+ enabled, set up the minimal required reserved power according to the class (*`Class 0`*..*`Class 4`*) of the powered device (PD).
  - If you know the exact maximum power consumption of a PD, you can additionally set the power limit for the given port to this known value.

Network availability aspects: Assign a PoE priority (*critical*, *high*, or *low*) to each PoE port. This helps deliver power to the most important PDs when the device is unable to deliver nominal power to all the connected PDs.

Energy conservation aspects:
- If you set the power limit for a given port to the known power consumption of the PD, this may help in powering more PDs simultaneously in certain cases.
- If you know the power consumption requirements of a PD on a time-of-day or day-of-week basis, you can activate the *Auto-shutdown power* function and set up the associated values *Disable power at [hh:mm]* and *Re-enable power at [hh:mm]*. The prerequisite for this is that the device system clock is synchronized to a reliable, trustworthy source.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Power over Ethernet" for setting up Power over Ethernet.

2.11.8 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.

2.11.9 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

2.11.10 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*
  The device loads the configuration profile from the external memory first.
  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 the external memory is *first* ⚠.

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to set the Configuration load priority for the external memory.

2.11.11 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.

2.11.12 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 75 “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.

2.11.13 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 75 “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.

2.11.14 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.

2.11.15 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
IEC 61850-MMS	Disabled	Disabled
Modbus TCP	Disabled	Disabled
EtherNet/IP	Disabled	Disabled
PROFINET	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.

2.11.16 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.

2.11.17 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.

2.11.18 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.

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.

2.11.19 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 42 "Planning a dedicated user account login policy").
For quantitative information on how to ensure a secure login policy (see on page 138 "Attack rate mitigation"). For quantitative information on how to help ensure hard-to-break passwords (see on page 125 "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.

2.11.20 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 43 “Planning a dedicated user account password policy”).
For quantitative information on how to help ensure hard-to-break passwords (see on page 125 “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 82 “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 84 “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.

2.11.21 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 45 “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 36 “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 36 “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.

2.11.22 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

2.11.23 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 50 "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

2.11.24 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

This enables the device to decide whether a TLS-based server it contacts is trustworthy or not.

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.

2.11.25 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 at rest), an appropriately secured remote destination may be preferable.

Note:
The Syslog client in the device offers unencrypted communication only.

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

2.11.26 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.

2.11.27 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 36 “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.

2.11.28 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

2.11.29 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.

2.11.30 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.

2.11.31 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.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - RADIUS (offers obfuscated communication)

Note:
The RADIUS 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 "Graphical User Interface" reference manual:
  - Chapter "Network Security > RADIUS" on how to set up the RADIUS client in the device

2.11.32 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 41 “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 72 “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 USB port
- To network ports or SFP slots
- Restrict physical (visual) access to the device LEDs and port LEDs.

2.12.1 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.

2.12.2 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.

2.12.3 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 121 “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 "Description > Ethernet ports" for the network ports
- Chapter "Installation > Connecting data cables" on details how to make data connections

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 94 “Device installation”)
- Device availability requirements (see on page 65 “Considering the device availability requirements”)
- Data connections (see on page 94 “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 56 “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 56 “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 121 “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 69 “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
- Connecting or removing a power supply
- Connecting or removing a PoE-/PoE+-powered device (PD) on a port **(depends on hardware)**

Note:
Depending on your system availability requirements, provide a redundant data upstream connection.
[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. Consider the new PoE/PoE+ power budget. Take the worst-case PoE/PoE+ power budget into account. If required, adapt the PoE/PoE+ parameters.

Refer to:
- The "Installation" user manual:
  - Chapter "Description > Ethernet ports" for the network ports
  - Chapter "Connecting data cables" on details how to make data connections
- The "Configuration" user manual:
  - Chapter "Configuring the ports > Enabling/disabling the port" for enabling or disabling a port
  - Chapter "Basic Settings > Power over Ethernet" for setting up PoE/PoE+ **(depends on hardware)**

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 53 “Develop a backup policy for device-related data”)
- According to your hardware replacement policy (see on page 53 “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 121 “Security seal”).
- ☐ On the new device, perform an initial software update (see on page 69 “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 72 “Security setup overview”).
  - If you have enabled configuration encryption (see on page 75 “Options to enable configuration encryption”).

- ☐ On the new device, restrict the hardware interfaces if required (see on page 92 “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 98 “Device hardware repair”).
  - If you want to decommission the device, follow your hardware decommissioning policy (see on page 100 “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 53 “Develop a policy for device hardware repair”).

Consider the following steps:

- ☐ Keep a backup copy of the device configuration (see on page 90 “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 100 “Deletion of confidential data and secrets”).
- ☐ Record the condition of the security seal on the device (see on page 121 “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 121 “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 75 “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 54 “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 101 “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 100 “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 121 “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 59 “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 25 “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 27 “Defense in depth vs. hardening”).
- Develop a general network mitigation strategy (see on page 30 “Developing a mitigation strategy”):
  - Collect the perceivable network mitigations.
  - Assess the network mitigation efficiency.
- Develop an individual mitigation strategy (see on page 33 “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 27 “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 72 “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 105 “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 105 “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.
- 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 the *HIPER Ring* 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 38 “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 47 “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.

3.4 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 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.

3.6 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 action:
  - Creating a log entry (only if assigned to an ingress port or a VLAN)

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 86 “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 only.
[CR2.11 RE1] Secure logging also relies on the synchronization of the device system clock to a trustworthy source (see on page 86 “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 122 “Glued front label”)
- Potted device (see on page 123 “Potted device”)
- Security stickers (see on page 123 “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 144 “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 130 "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 128 “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 141 “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 140 “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 134 “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 153 “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 150 “Key entry as ASCII string”).
- The policy strictly specifies a scheme (see on page 151 “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 133 “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 EtherNet/IP (setup) . . . 80
Access through IEC 61850-MMS (setup) . . . 80
Access through Modbus TCP (setup) . . . 80
Access through PROFINET (setup) . . . 80
Access to the system monitor through the serial port (setup) . . . 89
Acess Control Lists, setup details (network) . . . 112
ACL administration (network) . . . 115
ACL introduction (network) . . . 112
ACL planning (network) . . . 114
ACL setup (network) . . . 114
ACL setup details (network) . . . 112
ACL test (network) . . . 114
ACLs and their associations (network) . . . 113
Advanced user authentication (setup) . . . 90
Advanced user authentication measures (planning) . . . 48
Aggressive assumptions about attackers . . . 130
Alternatives to mitigation (planning) . . . 31
Approximations in this document (Planning) . . . 20
Assess mitigation measure efficiency (planning) . . . 30
Assess the individual threat risks (Planning) . . . 26
Assign IP address parameters to the device management (setup) . . . 74
Assumptions (aggressive) about attackers . . . 130
Assumptions (conservative) about the attack context . . . 131
Assumptions (conservative) about users . . . 130
Attack protection support functions (network) . . . 111
Attack rate mitigation . . . 138
Attack rate mitigation examples . . . 139
Attack resistance time (quantitative) . . . 137
Attack resistance time examples (mitigated attack rate) . . . 139
Attack resistance time examples (unmitigated attack rate) . . . 138
Attack strategies on passwords . . . 129
Audience of this document . . . 13
Audit trail (created by persistent logging) . . . 117
Authentication server considerations (planning) . . . 51

B

Backup of device-specific data (setup) . . . 90
Backup policy for device-related data (planning) . . . 53
Basic security - confidentiality example (Planning) . . . 19
Basic security assumptions for passwords . . . 130
Basics (Planning) . . . 15
Binary or continuous security viewpoints (planning) . . . 34

C

Calculating the required password entropy 142
Capability security levels (introduction) 22
Certificates and revocation lists (setup) 87
Checking the security seal (Maintenance) 96
Checking the security seal (Planning) 41
Checking the security seal (setup) 94
Choosing a secure installation location (setup) 65
CLI service shell, disable access (setup) 89
Combining threat risk and mitigation efficiency - criticality (planning) 33, 34
Compilininge a threat profile (Planning) 25
Configuration load priority (Planning) 40
Configuration load priority (Setup) 78
Conservative assumptions about the attack context 131
Conservative assumptions about users 130
Consider data link redundancy requirements (setup) 68
Consider device availability requirements (setup) 65
Consider power budget requirements (setup) 67
Consider power supply redundancy requirements (setup) 66
Considerations for manually generated keys 149
Create backup of device-specific data (setup) 90
Creating ACLs and associations (network) 113
Criticality - Combining threat risk and mitigation efficiency (planning) 33, 34
Criticality assessment and mitigation (Planning) 33

D

Data connections (installation) . . . 94
Data link redundancy requirements (considerations for setup) . . . 68
Decommissioning
Deletion of confidential data and secrets . . . 100
Delivery state, reset to . . . 100
Reset to the delivery state . . . 100
Secure physical destruction of device and possible accessories . . . 101
Decommissioning policy, device hardware (planning) . . . 54
Dedicated HTTPS certificate (setup) . . . 80
Dedicated login banners (setup) . . . 89
Dedicated SNMPv3 authentication and encryption password policy (setup) . . . 85
Dedicated SSH host key pair (setup) . . . 81
Dedicated user account login policy (setup) . . . 82
Dedicated user account password policy (setup) . . . 83
Dedicated user accounts and roles for device management (setup) . . . 84
Defense in depth (network) . . . 104
Defense in depth (system planning) . . . 27
Defense in depth (system planning), responsibilities . . . 28
Defense in depth example (planning) . . . 28
Defense in depth vs. hardening (planning) . . . 27
Defense in depth, detailed example (planning) . . . 29
Deletion of confidential data and secrets (decommissioning) . . . 100
Delivery state (Reset to, decommissioning) . . . 100
Detailed example of defense in depth (planning) . . . 29
Develop the device configuration (setup) . . . 59
Developing a mitigation strategy (planning) . . . 30
Developing a secure boot policy (Planning) . . . 42
Device and port LED visibility (planning) . . . 41
Device and port LEDs (restrict physical (visual) access, Security setup) . . . 93
Device availability (planning) . . . 40
Device decommissioning (overview) . . . 100
Device hardware decommissioning policy (planning) . . . 54
Device hardware interfaces (restrictions to, Security setup) . . . 92
Device hardware repair (maintenance) . . . 98
Device hardware repair policy (planning) . . . 53
Device hardware replacement (maintenance) . . . 97
Device hardware setup (installation) . . . 94
Device hardware, replacement policy (planning) . . . 53
Device installation . . . 94
Device security in the lifecycle phases (main chapter) . . . 59
Device-related data, backup policy (planning) . . . 53
Device-related policies (planning) . . . 53
DHCP server considerations (planning) . . . 50
Disable access (logical) to unused ports and SFP slots (setup) . . . 76
Disable access to the CLI service shell (setup) . . . 89
Disable automatic device software update from external memory (setup) . . . 77
Disable copying a file into the device without valid cryptographic signature (setup) . . . 78
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) (network) . . . 108
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) (network) . . . 106
Disable insecure management protocols (setup) . . . 79
Disable loading configuration profile without valid fingerprint (setup) . . . 79
Disable logical access to unused ports and SFP slots (setup) . . . 76
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP (network) . . . 108
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP (network) . . . 106
Disable SNMPv1 traps (setup) . . . 88
Disable writing unencrypted configuration profile to external memory (setup) . . . 79
Document the planned policies . . . 57

E
Enable SNMPv3 traps (setup) . . . 88
Entropy (password) . . . 141
Example (Planning) . . . 16
Example of defense in depth (planning) . . . 28
External authentication server considerations (planning) . . . 51
External DHCP server considerations (planning) . . . 50
External log server considerations (planning) . . . 52
External server considerations (planning) . . . 49

G
General vs. security-related device functions (setup) . . . 61

H
Harden your network (network) . . . 104
Hardening vs. defense in depth (planning) . . . 27
Hardware and setup scenarios, relationship . . . 24
Hardware changes (maintenance) . . . 96
Hardware vs. software measures (setup) . . . 60
Help secure the network protocols used (network) . . . 108
Help secure the redundancy protocols used (network) . . . 109
Helping secure the network infrastructure (network) . . . 105
HiDiscovery . . . 73
HiDiscovery (Setup) . . . 74
High-complexity passwords . . . 132
HiView . . . 69
HTTPS certificate (setup) . . . 80

I
Impact of device requirements on system planning . . . 39
Impact of external servers on system planning . . . 49
Impact of network aspects on system planning . . . 49
Impact of system lifecycle on the device lifecycle (planning) . . . 38
Impartial assessment (Planning) . . . 18
Industrial HiVision . . . 11
Installation
  Data connections . . . 94
  Device . . . 94
  Device hardware setup . . . 94
Intended audience of this document . . . 13
Introduction
  Capability security levels (SL-C) . . . 22
Introduction (network) . . . 103
Introduction (required preparatory work) . . . 22
Introduction to defense in depth (planning) . . . 27
IP access restrictions (setup) . . . 79
IP address parameters for the device management (setup) . . . 74

K
Key rotation . . . 50
Key strength (quantitative) . . . 149
Key strength example (optimistic) . . . 150, 151
Key strength example (skeptic) . . . 151, 152

L

LED visibility (device and port LEDs, planning) . . . 41
LEDs (restrict physical (visual) access, Security setup) . . . 93
Lifecycle phases for device security (main chapter) . . . 59
LLDP parameter planning (network) . . . 47
LLDP parameter setup (network) . . . 118
Log server considerations (planning) . . . 52
Logging (setup) . . . 88
Logging parameters (network) . . . 117
Logging policy (planning) . . . 47
Logical vs. physical measures (setup) . . . 60
Login banners (setup) . . . 89
Lookup tables for password policies (quantitative) . . . 144
Low-complexity passwords . . . 134

M

MAC address conflict detection (network) . . . 111
Maintenance
  Checking the security seal . . . 96
  Device hardware replacement . . . 97
  Hardware changes . . . 96
  Hardware repair . . . 98
  Software update . . . 96
Maintenance and operation policy (planning) . . . 56
Maintenance overview (setup) . . . 96
Management IP access restrictions (setup) . . . 79
Management VLAN (setup) . . . 76
Manually generated keys, considerations . . . 149
Measures to help secure the network infrastructure (network) . . . 105
Mitigation (attack rate) . . . 138
Mitigation efficiency value and unit (planning) . . . 31
Mitigation examples (attack rate) . . . 139
Mitigation strategy development (planning) . . . 30
Mitigation, alternatives (planning) . . . 31

N

Network
Acess Control Lists details (setup) . . . 112
ACL administration . . . 115
ACL introduction . . . 112
ACL planning . . . 114
ACL setup . . . 114
ACL setup details . . . 112
ACL test . . . 114
ACLs and their associations . . . 113
Attack protection support functions . . . 111
Audit trail (created by persistent logging) . . . 117
Creating ACLs and associations . . . 113
Defense in depth . . . 104
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 108
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) . . . 106
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP . . . 108
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP . . . 106
Harden your network . . . 104
Help secure the network protocols used . . . 108
Help secure the redundancy protocols used . . . 109
Helping secure the infrastructure . . . 105
Introduction . . . 103
LLDP parameter planning . . . 47
LLDP parameter setup . . . 118
Logging parameters . . . 117
MAC address conflict detection . . . 111
Measures to help secure the infrastructure . . . 105
Planning the LLDP parameters . . . 47
Port Security . . . 106
Potential conflicts of aims for an ACL . . . 113
Prerequisites . . . 103
Rate limiter . . . 111
Restrict logical access . . . 106
RSTP guards and helper protocols, set up . . . 109
Security support (by the device) . . . 103
Set up RSTP guards and helper protocols . . . 109
Set up the Denial of Service (DoS) parameters . . . 111
Set up the HIPER Ring parameters . . . 110
Set up the LLDP parameters . . . 118
Set up the logging parameters . . . 117
Set up the Media Redundancy Protocol (MRP) parameters . . . 110
Set up the MRP (Media Redundancy Protocol) parameters . . . 110
Set up the network time synchronization parameters . . . 116
Time Synchronization parameters . . . 116
VLAN segregation . . . 106
Network ports or SFP slots (restrict physical access) . . . 93
Network security support (by the device) . . . 103
Network time synchronization considerations (planning) . . . 50

O

Operation and maintenance policy (planning) . . . 56
Operation overview (setup) . . . 95
Overview (Planning) . . . 21
Overview (setup) . . . 72

P

Password and cryptographic key basics (planning) . . . 36
Password attack strategies . . . 129
Password classes . . . 125
Password entropy . . . 141
Password policies . . . 127
Password policy guide . . . 125
Password policy lookup tables (quantitative) . . . 144
Password schemes . . . 128
Password security assumptions . . . 130
Password strength . . . 125
Password strength (quantitative) . . . 132
Password strength example (high-complexity, optimistic) . . . 133
Password strength example (high-complexity, skeptic) . . . 134
Password strength example (low-complexity) . . . 136
Passwords (high-complexity) . . . 132
Passwords (low-complexity) . . . 134
Physical
  Restrict access to network ports or SFP slots (setup) . . . 93
  Restrict access to the device and port LEDs (setup) . . . 93
Physical vs. logical measures (setup) . . . 60
Planning
  Advanced user authentication measures . . . 48
  Alternatives to mitigation . . . 31
  Assess mitigation measure efficiency . . . 30
  Assess the individual threat risks . . . 26
  Authentication server considerations . . . 51
  Backup policy for device-related data . . . 53
  Basic mitigation - confidentiality example . . . 19
  Basics . . . 15
  Binary or continuous security viewpoints . . . 34
  Checking the security seal . . . 41
  Combining threat risk and mitigation efficiency - criticality . . . 33, 34
  Compiling a threat profile . . . 25
  Configuration load priority . . . 40
  Criticality - Combining threat risk and mitigation efficiency . . . 33, 34
  Criticality assessment and mitigation . . . 33
  Decommissioning policy, device hardware . . . 54
  Defense in depth . . . 27
  Defense in depth example . . . 28
  Defense in depth vs. hardening . . . 27
  Defense in depth, detailed example . . . 29
  Defense in depth, introduction . . . 27
  Defense in depth, purpose . . . 27
  Defense in depth, responsibilities . . . 28
  Detailed example of defense in depth . . . 29
  Developing a mitigation strategy . . . 30
  Developing a secure boot policy . . . 42
  Device and port LED visibility . . . 41
  Device availability . . . 40
  Device hardware decommissioning policy . . . 54
  Device hardware repair policy . . . 53
  Device hardware, replacement policy . . . 53
  Device-related data, backup policy . . . 53
  Device-related policies . . . 53
  DHCP server considerations . . . 50
  Document the planned policies . . . 57
  Example . . . 16
  Example of defense in depth . . . 28

External authentication server considerations . . . 51
External DHCP server considerations . . . 50
External log server considerations . . . 52
External server considerations . . . 49
Hardening vs. defense in depth . . . 27
Impact of device requirements on system . . . 39
Impact of external servers on the system . . . 49
Impact of network aspects on the system . . . 49
Impact of system lifecycle on device lifecycle . . . 38
Impartial assessment . . . 18
LED visibility (device and port LEDs) . . . 41
Log server considerations . . . 52
Logging policy . . . 47
Maintenance and operation policy . . . 56
Mitigation efficiency value and unit . . . 31
Mitigation strategy development . . . 30
Mitigation, alternatives . . . 31
Network time synchronization considerations . . . 50
Operation and Maintenance policy . . . 56
Overview . . . 21
Password and cryptographic key basics . . . 36
Port and device LED visibility . . . 41
Purpose of . . . 27
RADIUS server . . . 51
Redundancy protocols and VLANs . . . 47
Repair policy, device hardware . . . 53
Replacement policy for device hardware . . . 53
Residual risk . . . 34
Responsibilities for defense in depth . . . 28
Restrictions to the device hardware interfaces . . . 41
Risk value and unit . . . 25
Scenario development . . . 24
Secure installation location . . . 39
Security terminology . . . 15
Security terminology, more . . . 16
Security viewpoints (binary or continuous) . . . 34
Session timeouts . . . 46
Skepticism vs. optimism . . . 18
SNMPv3 authentication and encryption password . . . 46
Software auto update . . . 40
Software update and configuration server considerations . . . 49
SSH key auto upload . . . 40
Strategies to improve security . . . 20
Tension of convenience vs. security . . . 17
Theoretical and practical degrees of security . . . 20
Threat analysis . . . 19
Unsigned device software, upload . . . 42
Upload of unsigned device software . . . 42
User account and role policy for device management . . . 45
User account login policy . . . 42
User account password policy . . . 43
VLAN . . . 38
VLANs and redundancy protocols . . . 47
Planning for security . . . 15
Planning the LLDP parameters (network) . . . 47
PoE (setup) (depends on hardware) . . . 76
Port and device LED visibility (planning) . . . 41
Port and device LEDs (restrict physical (visual) access, Security setup) . . . 93
Port Security (network) . . . 106

Possible further prerequisites (setup overview) . . . 62
Potential conflicts of aims for an ACL (network) . . . 113
Power over Ethernet (setup) (depends on hardware) . . . 76
Preparation for installation, suggested (Setup) . . . 63
Preparatory work (introduction) . . . 22
Prerequisites (network) . . . 103
Prerequisites for installation and setup (setup overview) . . . 62
Purpose of defense in depth (planning) . . . 27

Q

Quantitative key strength . . . 149
Quantitative password strength . . . 132

R

RADIUS client (Setup) . . . 90
RADIUS server (Planning) . . . 51
Rate limiter (network) . . . 111
Reasons for suggested installation step sequence (setup) . . . 63
Recommended work step sequence (Setup overview) . . . 63
Redundancy protocols and VLANs (planning) . . . 47
Relationship of hardware and setup scenarios . . . 24
Repair policy, device hardware (planning) . . . 53
Replacement policy for device hardware (planning) . . . 53
Required attack resistance time (quantitative) . . . 140
Required password entropy (calculation) . . . 142
Required preparatory work (introduction) . . . 22
Reset to the delivery state (decommissioning) . . . 100
Residual risk (planning) . . . 34
Responsibilities for defense in depth (system planning) . . . 28
Restrict access to network ports or SFP slots (physical, Security setup) . . . 93
Restrict access to the device and port LEDs (physical, Security setup) . . . 93
Restrict access to USB port (physical, security setup) . . . 92
Restrict logical access (network) . . . 106
Restrictions to device hardware interfaces (setup) . . . 92
Restrictions to the device hardware interfaces (planning) . . . 41
Risk value and unit (planning) . . . 25
RSTP guards and helper protocols (network, set up) . . . 109

S

Scenario development (planning) . . . 24
Scenarios (Relationship of hardware and setup scenarios) . . . 24
Scope of this document . . . 21
Secure installation location (planning) . . . 39
Secure physical destruction of device and possible accessories (decommissioning) . . . 101
Security assumptions for passwords . . . 130
Security levels (SL-C, introduction) . . . 22
Security planning . . . 15
Security seal . . . 121
Security seal details . . . 121, 122
Security seal overview . . . 121
Security setup overview . . . 72
Security terminology (Planning) . . . 15
Security terminology, more (Planning) . . . 16
Security viewpoints (binary or continuous, planning) . . . 34
Security-related vs. general device functions (setup) . . . 61
Server key rotation . . . 50
Session timeouts (planning) . . . 46
Set up device time synchronization (setup) . . . 86
Set up RSTP guards and helper protocols (network) . . . 109
Set up the Denial of Service (DoS) parameters (network) . . . 111
Set up the HIPER Ring parameters (network) . . . 110
Set up the LLDP parameters (network) . . . 118
Set up the logging parameters (network) . . . 117
Set up the MRP (Media Redundancy Protocol) parameters (network) . . . 110
Set up the network time synchronization parameters (network) . . . 116
Set up the SSH Known Hosts fingerprints (setup) . . . 82
Set up the the Media Redundancy Protocol (MRP) parameters (network) . . . 110
Set up time synchronization (setup) . . . 86
Setting of secure boot mode (setup) . . . 75
Setup
- Access through EtherNet/IP . . . 80
- Access through IEC 61850-MMS . . . 80
- Access through Modbus TCP . . . 80
- Access through PROFINET . . . 80
- Access to the system monitor through the serial port . . . 89
- Advanced user authentication . . . 90
- Assign IP address parameters for the device management . . . 74
- Backup of device-specific data . . . 90
- Certificates and revocation lists . . . 87
- Checking the security seal . . . 94
- Choosing a secure installation location . . . 65
- CLI service shell, disable access . . . 89
- Configuration load priority . . . 78
- Consider data link redundancy requirements . . . 68
- Consider device availability requirements . . . 65
- Consider power budget requirements . . . 67
- Consider power supply redundancy requirements . . . 66
- Create backup of device-specific data . . . 90
- Data link redundancy requirements . . . 68
- Dedicated HTTPS certificate . . . 80
- Dedicated login banners . . . 89
- Dedicated SNMPv3 authentication and encryption password policy . . . 85
- Dedicated SSH host key pair . . . 81
- Dedicated user account login policy . . . 82
- Dedicated user account password policy . . . 83
- Dedicated user accounts and roles for device management . . . 84
- Develop the device configuration . . . 59

Device hardware . . . 94
Device hardware interfaces (restrictions to) . . . 92
Device time synchronization . . . 86
Disable access (logical) to unused ports and SFP slots . . . 76
Disable access to the CLI service shell . . . 89
Disable automatic device software update from external memory . . . 77
Disable copying a file into the device without valid cryptographic signature . . . 78
Disable insecure management protocols . . . 79
Disable loading configuration profile without valid fingerprint . . . 79
Disable logical access to unused ports and SFP slots . . . 76
Disable SNMPv1 traps . . . 88
Disable writing unencrypted configuration profile to external memory . . . 79
Enable SNMPv3 traps . . . 88
General vs. security-related device functions . . . 61
Hardware vs. software measures . . . 60
HiDiscovery . . . 74
HTTPS certificate . . . 80
IP access restrictions . . . 79
IP address parameters for the device management . . . 74
Logging . . . 88
Logical vs. physical measures . . . 60
Login banners . . . 89
Maintenance overview . . . 96
Management IP access restrictions . . . 79
Management VLAN . . . 76
Operation overview . . . 95
Physical vs. logical measures . . . 60
PoE (depends on hardware) . . . 76
Power over Ethernet (depends on hardware) . . . 76
Preparation for installation, suggested . . . 63
Prerequisites for installation and setup . . . 62
RADIUS client . . . 90
Reasons for suggested installation step sequence . . . 63
Restrict physical access to USB port . . . 92
Restrictions to device hardware interfaces . . . 92
Security-related vs. general device functions . . . 61
Set up the SSH Known Hosts fingerprints . . . 82
Setting of secure boot mode . . . 75
SNMPv1 traps . . . 88
SNMPv3 authentication and encryption password policy . . . 85
SNMPv3 traps . . . 88
Software update . . . 69
Software vs. hardware measures . . . 60
Specify finite session timeouts . . . 86
SSH host key pair . . . 81
SSH key auto upload . . . 77
Suggested installation step sequence (reasons for) . . . 63
Suggested preparation for installation . . . 63
System monitor, Access through the serial port . . . 89
Time synchronization . . . 86
USB port (restrict physical access) . . . 92
User account login policy . . . 82
User account password policy . . . 83
User accounts and roles for device management . . . 84
VLAN dedicated to management access . . . 76
Setup overview . . . 72
Setup overview (Possible further prerequisites) . . . 62
SFP slots or network ports (restrict physical access) . . . 93
Skepticism (Basic approximations) . . . 20

Skepticism (Planning) . . . 20
Skepticism vs. optimism (Planning) . . . 18
SL-C (introduction) . . . 22
SNMPv1 traps (setup) . . . 88
SNMPv3 authentication and encryption password (planning) . . . 46
SNMPv3 authentication and encryption password policy (setup) . . . 85
SNMPv3 traps (setup) . . . 88
Software auto update (Planning) . . . 40
Software update (maintenance) . . . 96
Software update (setup) . . . 69
Software update and configuration server considerations (Planning) . . . 49
Software vs. hardware measures (setup) . . . 60
Specify finite session timeouts (setup) . . . 86
SSH host key pair (setup) . . . 81
SSH key auto upload (Planning) . . . 40
SSH key auto upload (Setup) . . . 77
SSH server key rotation . . . 50
Strategies to improve security (Planning) . . . 20
Subject of this document . . . 21
Suggested installation step sequence (reasons for, setup) . . . 63
Suggested preparation for installation (Setup) . . . 63
Summary of this document . . . 13
Synopsis of this document . . . 13
System monitor, Access through the serial port (setup) . . . 89

T

Technical Documents . . . 167
Technical questions . . . 167
Technical Support . . . 167
Tension of convenience vs. security (Planning) . . . 17
Theoretical and practical degrees of security (Planning) . . . 20
Threat analysis (Planning) . . . 19
Time Synchronization parameters (network) . . . 116
Training courses . . . 167

U

Unsigned device software, upload (Planning) . . . 42
Upload of unsigned device software (Planning) . . . 42
USB port (restrict physical access, security setup) . . . 92
User account and role policy for device management (planning) . . . 45
User account login policy (planning) . . . 42
User account login policy (setup) . . . 82
User account password policy (planning) . . . 43
User account password policy (setup) . . . 83
User accounts and roles for device management (setup) . . . 84

V

VLAN (planning) . . . 38
VLAN dedicated to management access (setup) . . . 76
VLAN segregation (network) . . . 106
VLANs and redundancy protocols (planning) . . . 47

W

Work step sequence (recommended, Setup overview) . . . 63

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