



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

GRS103 HiOS-2A Rel. 10200

Reference Manual
Graphical User Interface

User Manual
Configuration



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

Graphical User Interface
GREYHOUND Switch GRS103
HiOS-2A

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

© 2025 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
	Banner	11
	Menu pane	13
	Dialog area	15
1	Basic Settings	19
1.1	System	19
1.2	Modules	24
1.3	Network	26
1.3.1	Global	27
1.3.2	IPv4	29
1.3.3	IPv6	32
1.4	Out-of-Band over USB	36
1.5	Software	38
1.6	Load/Save	42
1.7	External Memory	54
1.8	Port	57
1.9	Power over Ethernet	63
1.9.1	PoE Global	64
1.9.2	PoE Port	66
1.10	Restart	69
2	Time	73
2.1	Basic Settings	73
2.2	SNTP	77
2.2.1	SNTP Client	78
2.2.2	SNTP Server	82
3	Device Security	85
3.1	User Management	85
3.2	Authentication List	91
3.3	LDAP	93
3.3.1	LDAP Configuration	94
3.3.2	LDAP Role Mapping	100
3.4	Management Access	102
3.4.1	Server	103
3.4.2	IP Access Restriction	116
3.4.3	Web	119
3.4.4	Command Line Interface	120
3.4.5	SNMPv1/v2 Community	122
3.5	Pre-login Banner	124

3.6	SSH Known Hosts	125
4	Network Security	129
4.1	Network Security Overview	129
4.2	Port Security	131
4.3	802.1X	136
4.3.1	802.1X Global	137
4.3.2	802.1X Port Configuration	139
4.3.3	802.1X Port Clients	145
4.3.4	802.1X EAPOL Port Statistics	147
4.3.5	802.1X Port Authentication History	149
4.3.6	802.1X Integrated Authentication Server (IAS)	151
4.4	RADIUS	152
4.4.1	RADIUS Global	153
4.4.2	RADIUS Authentication Server	155
4.4.3	RADIUS Accounting Server	157
4.4.4	RADIUS Authentication Statistics	159
4.4.5	RADIUS Accounting Statistics	161
4.5	DoS	162
4.5.1	DoS Global	163
4.6	ACL	166
4.6.1	ACL IPv4 Rule	167
4.6.2	ACL MAC Rule	171
4.6.3	ACL Assignment	174
5	Switching	177
5.1	Switching Global	177
5.2	Rate Limiter	180
5.3	Filter for MAC Addresses	183
5.4	IGMP Snooping	185
5.4.1	IGMP Snooping Global	186
5.4.2	IGMP Snooping Configuration	188
5.4.3	IGMP Snooping Enhancements	192
5.4.4	IGMP Snooping Querier	195
5.4.5	IGMP Snooping Multicasts	198
5.5	MRP-IEEE	199
5.5.1	MRP-IEEE Configuration	200
5.5.2	MRP-IEEE Multiple MAC Registration Protocol	201
5.5.3	MRP-IEEE Multiple VLAN Registration Protocol	206
5.6	GARP	209
5.6.1	GMRP	210
5.6.2	GVRP	212
5.7	QoS/Priority	213
5.7.1	QoS/Priority Global	214
5.7.2	QoS/Priority Port Configuration	215
5.7.3	802.1D/p Mapping	217
5.7.4	IP DSCP Mapping	218
5.7.5	Queue Management	220

5.8	VLAN	221
5.8.1	VLAN Global	222
5.8.2	VLAN Configuration	223
5.8.3	VLAN Port	226
5.8.4	VLAN Voice	228
5.9	L2-Redundancy	230
5.9.1	MRP	231
5.9.2	Spanning Tree	235
5.9.2.1	Spanning Tree Global	236
5.9.2.2	Spanning Tree Port	242
5.9.3	Link Aggregation	249
5.9.4	Link Backup	255
5.9.5	FuseNet	258
5.9.5.1	Sub Ring	259
5.9.5.2	Ring/Network Coupling	264
6	Diagnostics	271
6.1	Status Configuration	271
6.1.1	Device Status	272
6.1.2	Security Status	277
6.1.3	Signal Contact	284
6.1.3.1	Signal Contact 1 / Signal Contact 2	285
6.1.4	MAC Notification	290
6.1.5	Alarms (Traps)	292
6.1.5.1	Trap V3 User Management	293
6.1.5.2	Trap Destinations	296
6.2	System	298
6.2.1	System Information	299
6.2.2	Hardware State	300
6.2.3	Configuration Check	301
6.2.4	IP Address Conflict Detection	303
6.2.5	ARP	307
6.2.6	Selftest	309
6.3	Email Notification	311
6.3.1	Email Notification Global	312
6.3.2	Email Notification Recipients	317
6.3.3	Email Notification Mail Server	319
6.4	Syslog	321
6.5	Ports	326
6.5.1	SFP	327
6.5.2	TP cable diagnosis	328
6.5.3	Port Monitor	330
6.5.4	Auto-Disable	340
6.5.5	Port Mirroring	344
6.6	LLDP	346
6.6.1	LLDP Configuration	347
6.6.2	LLDP Topology Discovery	351

6.7	Loop Protection	355
6.8	Report	359
6.8.1	Report Global	360
6.8.2	Persistent Logging	364
6.8.3	System Log	367
6.8.4	Audit Trail	368
7	Advanced	369
7.1	DHCP	369
7.1.1	DHCP Server	369
7.1.1.1	DHCP Server Global	370
7.1.1.2	DHCP Server Pool	372
7.1.1.3	DHCP Server Lease Table	377
7.2	DHCP L2 Relay	378
7.2.1	DHCP L2 Relay Configuration	379
7.2.2	DHCP L2 Relay Statistics	382
7.3	DNS	383
7.3.1	DNS Client	383
7.3.1.1	DNS Client Global	384
7.3.1.2	DNS Client Current	385
7.3.1.3	DNS Client Static	386
7.3.1.4	DNS Client Static Hosts	389
7.4	Industrial Protocols	390
7.4.1	IEC61850-MMS	391
7.4.2	Modbus TCP	394
7.4.3	OPC UA Server	396
7.4.4	Service Discovery	399
7.5	Tracking	401
7.5.1	Tracking Configuration	402
7.5.2	Tracking Applications	406
7.6	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 contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

Key

The designations used in this manual have the following meanings:

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

 Execution in the Graphical User Interface

 Execution in the Command Line Interface

Notes on the Graphical User Interface

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

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

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

The Graphical User Interface is divided as follows:

- [Banner](#)
- [Menu pane](#)
- [Dialog area](#)

Banner

The banner displays the following information:



Displays and hides the menu. When the web browser window is too narrow, the Graphical User Interface hides the menu pane. The banner displays the button instead.

Brand logo

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

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

Menu pane

When the web browser window is too narrow, the Graphical User Interface hides the menu pane.

To display the menu pane, click the  button in the banner.

The menu pane is divided as follows:

- [Icons bar](#)
- [Menu tree](#)

Icons bar

The icons bar displays the following information:


Device software

Displays the version number of the 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.



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



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

Menu tree

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



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



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

Dialog area

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

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

- [Control elements](#)
- [Modification mark](#)
- [Standard buttons](#)
- [Saving the settings](#)
- [Updating the display](#)
- [Working with tables](#)

Control elements

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

The control elements have the following visual properties:

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

Modification mark

When you modify a value, the corresponding field or table cell displays a red triangle in its top-left corner. The red triangle indicates that you have not yet 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.



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

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



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

Click the icon to sort the table rows in 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.



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

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

Selecting multiple table rows

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

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

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

Once you have selected multiple table rows, you can apply an action to each of these table rows at the same time, for example:

- Entering or changing the values in one table column
- Removing multiple table rows

1 Basic Settings

The menu contains the following dialogs:

- [System](#)
- [Modules](#)
- [Network](#)
- [Out-of-Band 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 2 redundant power supply units, then the device triggers an alarm. To avoid this alarm, deactivate the monitoring of the missing power supply units in the [Diagnostics > Status Configuration > Device Status](#) dialog.

Security status



Security status

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

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

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

Signal contact status

The device can contain several signal contacts.



Signal contact status

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

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

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

System data

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

System name

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

Possible values:

Alphanumeric ASCII character string with 0..255 characters

The device accepts the following characters:

- 0 . 9
 - a . z
 - A . Z
 - ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~
- <device type name>-<MAC address> (default setting)

When generating an digital certificate, the application generating the certificate uses the specified value as the domain name and common name.

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

- DHCP client
- [Syslog](#)
- [IEC61850-MMS](#)

Location

Specifies the current or planned location.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Contact person

Specifies the contact person for this device.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Device type

Displays the product name of the basic device.

Power supply 1 Power supply 2

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

Possible values:

[present](#)
[defect i ve](#)
[not i nstal led](#)
[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



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



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

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

ACA



No external memory is connected.




The external memory is connected but not ready for operation.



The external memory is connected and ready for operation.

Port status

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

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

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

Green background color

Port with an active link.

Gray background color

Port with an inactive link.

Yellow background color

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

Dashed border

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

1.2 Modules

[Basic Settings > Modules]

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

As long as the *Ethernet module status* column displays the value *configurable*, you can set up the module and save its preferences.


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

Install an Ethernet module


Perform the following steps:

Plug the module in the slot.

The device automatically sets up the module with the default settings, and detects the module parameters.

To update the Graphical User Interface, click the  button.

The *Ethernet module status* column displays the value *physical* for the installed Ethernet module.

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

Activate/Deactivate a slot

On an inactive slot, the device recognizes the installed module and lets you set up the ports. The module establishes no network connections on an inactive slot.

Perform the following steps:

Select the table row of the module.

To deactivate the slot and deny network access, unmark the *Active* checkbox.

To activate the slot and allow network access, mark the *Active* checkbox.

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

Remove an Ethernet module

Perform the following steps:

Remove the module from the slot.

To update the Graphical User Interface, click the  button.

The *Ethernet module status* column displays the value *configurable* for the removed module.


Select the table row of the removed module.

Click the  button.

The *Ethernet module status* column displays the value *remove* for the removed module.

The *Type* column and some other columns display the value *n/a*.

The marked *Active* checkbox indicates that the slot is still active.

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

Table

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

Buttons



Removes the selected Ethernet module from the table.

Ethernet module

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

Active

Activates/deactivates the slot.

Possible values:

[marked](#) (default setting)

The slot is active. The device recognizes the module installed in this slot.

[unmarked](#)

The slot is inactive.

Type

Displays the type of the installed module.

A value of [n/a](#) indicates that the slot is empty.

Description

Specifies a short description of the installed module.

Version

Displays the version of the installed module.

Ports

Displays the number of ports that are available on the installed module.

Serial number

Displays the serial number of the installed module.

A value of [n/a](#) indicates that the slot is empty.

Ethernet module status

Displays the status of the slot.

Possible values:

[physical](#)

A module is present in the slot.

[configurable](#)

The slot is empty and available for setup.

[remove](#)

The slot is empty and inactive.

[fix](#)

The module cannot be removed.

1.3 Network

[Basic Settings > Network]

The menu contains the following dialogs:

- [Global](#)
- [IPv4](#)
- [IPv6](#)

1.3.1 Global

[Basic Settings > Network > Global]

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

Management interface

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

MAC address

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

HiDiscovery protocol v1/v2

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

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

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

Operation

Enables/disables the HiDiscovery function in the device.

Possible values:

On (default setting)

The HiDiscovery function is enabled.

You can use the HiDiscovery software to access the device from your PC.

Off

The HiDiscovery function is disabled.

Access

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

Possible values:

`readWrite` (default setting)

The HiDiscovery function has write access to the device. The device lets you change the IP parameters in the device using the HiDiscovery function.

`readOnly`

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

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

Signal

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

Possible values:

`marked`

The flashing of the port LEDs is active.

The port LEDs flash until you disable the function again.

`unmarked` (default setting)

The flashing of the port LEDs is inactive.

1.3.2 IPv4

[Basic Settings > Network > IPv4]

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

Configuration

IP address assignment

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

Possible values:

Local

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

BOOTP

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

DHCP (default setting)

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

When the server also provides the addresses of DNS servers, the device displays these addresses in the *Advanced > DNS > Client > Current* dialog.

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

Management interface

VLAN ID

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

Possible values:

1..4042 (default setting: 1)

The prerequisite is that in the *Switching > VLAN > Configuration* dialog the VLAN is already set up.

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

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

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

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.

1.3.3 IPv6

[Basic Settings > Network > IPv6]

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

Operation

Operation

Enables/disables the IPv6 protocol in the device.

You can operate IPv4 and IPv6 simultaneously in the device. This is possible with the use of the Dual IP Layer technique, also referred to as Dual Stack.

Possible values:

On (default setting)

IPv6 is enabled.

Off

IPv6 is disabled.

If you want the device to operate only using IPv4, then disable IPv6 in the device.

Configuration

Dynamic IP address assignment

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

Possible values:

None

The device receives its IPv6 parameters manually.

You can manually specify a maximum number of 4 IPv6 addresses. You cannot specify loopback, link-local, and Multicast addresses as static IPv6 addresses.

Auto (default setting)

The device receives its IPv6 parameters dynamically. The device receives a maximum of 2 IPv6 addresses.

An example here is the Router Advertisement Daemon (radvd). The radvd uses *Router Solicitation* and *Router Advertisement* messages to automatically set up an IPv6 address. The *Router Solicitation* and *Router Advertisement* messages are described in RFC 4861.

DHCPv6

The device receives its IPv6 parameters from a DHCPv6 server.

All

If the *All* radio button is selected, then the device receives its IPv6 parameters using every alternative for both dynamic and manual assignments.

Management interface

VLAN ID

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

Possible values:

1..4042 (default setting: 1)

The prerequisite is that in the [Switching > VLAN > Configuration](#) dialog the VLAN is already set up.

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

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

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

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://[<i>pv6_address</i>]`.

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

EUI option

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

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

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

Possible values:

marked

The *EUI option* function is active.

unmarked (default setting)

The *EUI option* function is inactive.

Origin

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

Possible values:

Autoconf

The device received the IPv6 address dynamically, when the *Auto* radio button is selected.

Manual

The device received the IPv6 address manually.

DHCP

The device received the IPv6 address from a DHCPv6 server.

Linklayer

The device automatically sets up a link-local type IPv6 address. The link-local address cannot be changed.

Status

Displays the current status of the IPv6 address.

Possible values:

active

The IPv6 address is active.

notInService

The IPv6 address is inactive.

notReady

The IPv6 address is specified, but not currently active as some configuration parameters are still missing.

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

1.4 Out-of-Band 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](#))

1.5 Software

[Basic Settings > Software]

This dialog lets you update the device software and display information about the device software.

You also have the option to restore a backup of the device software that is saved in the device.

Note: Before you update the device software, follow the version-specific notes in the [Readme](#) text file.

Version

Stored version

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

Running version

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

Backup version

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

Restore

The device swaps the device software images and accordingly the values displayed in the fields [Stored version](#) and [Backup version](#).

During the next system startup, the device loads the device software displayed in the [Stored version](#) field.

Bootcode

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

Software update


The device lets you update the device software at this place, if a suitable device software image is available outside the device. If a suitable device software image is saved on the selected external memory, 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 from an FTP server

This option is not recommended 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 from a TFTP server

This option is not recommended 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 from an SCP or SFTP server

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://<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 10.0.00.
- The *Allow upload of unsigned device software* checkbox is permanently hidden.

unmarked (default setting)

During system startup, the device boots with any device software image, whether the device software image is cryptographically signed or not. However, in case of a cryptographically signed device software image, its signature has to be valid.

[File system]

Table

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

Buttons

Update Firmware

Updates the device software if a suitable device software image is saved on the external memory. 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:

[r am](#)

Volatile memory of the device

[f l ash](#)

Non-volatile memory (NVM) of the device

[usb](#)

External USB memory (ACA21/ACA22)

Index

Displays the index of the device software.

The index number of the device software in the flash memory has the following meaning:

- [1](#)
During the next system startup, the device loads this device software.
- [2](#)
The device copied this device software into the backup area during the last software update.

File name

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

Firmware

Displays the version number and creation date of the device software.

1.6 Load/Save

[Basic Settings > Load/Save]

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

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

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

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

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

Table

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

Buttons



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

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



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.



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).

In the [Profile name](#) field, enter the name under which you want to save the configuration profile.

To save the configuration profile under a new name, click the **+** button.

To overwrite an existing configuration profile, select the corresponding item from the drop-down list.

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

Note: Before 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 default settings or terminates the restart and stops.

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

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

Import...

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

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

From the *Select source* drop-down list, select from where the device imports the configuration profile.

PC/URL


The device imports the configuration profile from the local PC or from a remote server.

External memory

The device imports the configuration profile from the external memory.

When **PC/URL** is selected above, in the *Import profile from PC/URL* frame you specify the configuration profile file to be imported.

- Import from the PC

If the file is on your PC or on a network drive, then drag and drop the file into the  area.

As an alternative, click in the area to select the file.

- Import from an FTP server

This option is not recommended 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 from a TFTP server

This option is not recommended 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 from an SCP or SFTP server

If the file is on an SCP or SFTP server, then specify the URL in one of the following forms:

`scp://` or `sftp://<IP address>/<path>/<file name>`

Click the *Start* button to open the *Credentials* window. In this window, you enter the *User name* and *Password* to log into the server.

`scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

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

When **External memory** is selected above, in the *Import profile from external memory* frame you specify the configuration profile file to be imported.

From the *Profile name* drop-down list, select the name of the configuration profile to be imported.

In the *Destination* frame you specify where the device saves the imported configuration profile.

In the *Profile name* field you specify the name under which the device saves the configuration profile.

In the *Storage* field you specify the storage location for the configuration profile. The prerequisite is that from the *Select source* drop-down list the **PC/URL** item is selected.

RAM

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

NVM

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

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

- If the configuration profile was exported on the same device or on an identically equipped device of the same type, then:
The device takes over the settings completely.
If the device uses modules, then also read the help text of the [Basic Settings > Modules](#) dialog.
- If the configuration profile was exported on an other device, then:
The device takes over the settings which it can interpret based on its hardware equipment and software level.
The remaining settings the device takes over from its `running-config` configuration profile.

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

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

Export...

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

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

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

- Export to an FTP server
This option is not recommended 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 to a TFTP server
This option is not recommended 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 to an SCP or SFTP server
To save the file on an SCP or SFTP server, specify the URL for the file in one of the following forms:
`scp://` or `sftp://<IP address>/<path>/<file name>`
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

If the file is on your PC or on a network drive, then drag and drop the file into the  area. As an alternative, click in the area to select the file.

- Import from an FTP server

This option is not recommended 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 from a TFTP server

This option is not recommended 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 from an SCP or SFTP server

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 settings in the device to the default values.

- The device deletes the saved configuration profiles from the volatile memory (**RAM**) and from the non-volatile memory (**NVM**).
- The device deletes the 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 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.

ENMM (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.

Possible values:

`usb`

External USB memory (ACA21/ACA22)

Status

Displays the operating state of the external memory.

Possible values:

`notPresent`

No external memory is connected.

`removed`

Someone has removed the external memory from the device during operation.

`ok`

The external memory is connected and ready for operation.

`outOfMemory`

The memory space is occupied in the external memory.

`genericErr`

The device has detected an error.

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.

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 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. The device copies the settings into the volatile memory (RAM) and into the non-volatile memory (NVM).

Delete

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

In the *Old password* field, enter the existing password.

To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox.

Mark the *Save configuration afterwards* checkbox to remove the encryption also for the “Selected” configuration profile in the non-volatile memory (NVM) and in the external memory.

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

Undo configuration modifications

Operation

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

Possible values:

On

The function is enabled.

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

Off (default setting)

The function is disabled.

Disable the function again before you close the Graphical User Interface. You thus help prevent the device from restoring the configuration profile designated as “Selected”.

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

Timeout [s] to recover after connection loss

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

Possible values:

30 . 600 (default setting: 600)

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

Watchdog IP address

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

Possible values:

IPv4 address (default setting: 0.0.0.0)

Information

NVM in sync with running config


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

Possible values:

marked

The settings match.

unmarked

The settings differ. Additionally, the Banner displays the icon .

External memory in sync with NVM

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

Possible values:

marked

The settings match.

unmarked

The settings differ.

Possible causes:

- No external memory is connected to the device.
- In the *Basic Settings > External Memory* dialog, the *Backup config when saving* function is disabled.

Backup config on a remote server when saving

Operation

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

Possible values:

Enabled

The *Backup config on a remote server when saving* function is enabled.

When you save the configuration profile in the non-volatile memory (NVM), the device automatically backs up the configuration profile on the remote server specified in the *URL* field.

Disabled (default setting)

The *Backup config on a remote server when saving* function is disabled.

URL

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

Possible values:

Alphanumeric ASCII character string with 0..128 characters

Example: `ftp://192.9.200.1/config.xml`

The device supports the following wildcards:

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

Set credentials

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

In the *User name* field, enter the user name.

To display the user name in plain text instead of ***** (asterisks), mark the *Display content* checkbox.

Possible values:

Alphanumeric ASCII character string with 1..32 characters

In the *Password* field, enter the password.

To display the password in plain text instead of ***** (asterisks), mark the *Display content* checkbox.

Possible values:

Alphanumeric ASCII character string with 6..64 characters

The device accepts the following characters:

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

1.7 External Memory

[Basic Settings > External Memory]

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

Table

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

Type

Displays the type of the external memory.

Possible values:

[usb](#)
External USB memory (ACA21/ACA22)

Status

Displays the operating state of the external memory.

Possible values:

[not Present](#)
No external memory is connected.
[removed](#)
Someone has removed the external memory from the device during operation.
[ok](#)
The external memory is connected and ready for operation.
[out Of Memory](#)
The memory space is occupied in the external memory.
[generi cErr](#)
The device has detected an error.

Writable

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

Possible values:

[marked](#)
The device has write access to the external memory.
[unmarked](#)
The device has read-only access to the external memory. Possibly the write protection is activated in the external memory.

Software auto update

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

Possible values:

marked (default setting)

The device updates the device software when the following files are located in the external memory:

- the 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 an external memory during the system startup.

Possible values:

marked (default setting)

The loading of the RSA key is activated.

During the system startup, the device loads the RSA key from the external memory when the following files are located in the external memory:

- SSH RSA key file
- a text file `startup.txt` with the content `autoUpdateRSA=<filename_of_the_SSH_RSA_key>`

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

unmarked

The loading of the RSA key is deactivated.

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

Config priority

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

Possible values:

disable

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

first

The device loads the configuration profile from the external memory.

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

Note: When loading the configuration profile from the external memory (**EMM**), 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.

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.

unmarked

Saving a copy is deactivated. The device does not save a copy of the configuration profile.

Manufacturer ID

Displays the name of the memory manufacturer.

Revision

Displays the revision number specified by the memory manufacturer.

Version

Displays the version number specified by the memory manufacturer.

Name

Displays the product name specified by the memory manufacturer.

Serial number

Displays the serial number specified by the memory manufacturer.

1.8 Port

[Basic Settings > Port]

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

The dialog contains the following tabs:

- [\[Configuration\]](#)
- [\[Statistics\]](#)
- [\[Ingress Utilization\]](#)

[Configuration]

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 and the media module used.

Link/Current settings

Displays the operating mode which the port currently uses.

Possible values:

- No cable connected, no link.
- 10M 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 and the media module used.

Manual cable crossing

Specifies the devices connected to a twisted-pair port.

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

Possible values:

- mdi*
The device interchanges the send- and receive-line pairs on the port.
- mdi x* (default setting on twisted-pair ports)
The device helps prevent the interchange of the send- and receive-line pairs on the port.
- auto-mdi x*
The device detects the send and receive line pairs of the connected device and automatically adapts to them.
Example: When you connect an end device with a crossed cable, the device automatically resets the port from *mdi x* 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 you deactivate the flow control on the participating ports. If the flow control and the redundancy function are active at the same time, it is possible that the redundancy function operates differently than intended.

Send trap

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.

Power state

Specifies if the port is physically enabled or disabled after you deactivated the port in the [Port on](#) column.

Possible values:

marked

The device keeps the port physically enabled when the [Port on](#) checkbox is unmarked. A device connected to this port continues to detect the link status as active.

unmarked (default setting)

The port is physically disabled. The physical status of the port is controlled only by the setting in the [Port on](#) column.

Track name

Displays the name of the tracking object made up of the values displayed in the [Type](#) and [Track ID](#) columns.

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.

1.9 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](#)

1.9.1 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.

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:

[i n t e r n a l](#)

Internal power source

[e x t e r n a l](#)

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:

[m a r k e d](#) (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.

[u n m a r k e d](#)

The sending of SNMP traps is inactive.

1.9.2 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:

- [Class 0](#)
- [Class 1](#)
- [Class 2](#)
- [Class 3](#)
- [Class 4](#)

Class 0
Class 1
Class 2
Class 3
Class 4

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

Possible values:

- [marked](#) (default setting)
- [unmarked](#)

Consumption [W]

Displays the current power consumption of the port in watts.

Possible values:

0, 0 . 30, 0

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, 0 . 30, 0 (default setting: 0)

Max. consumption [W]

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

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

Name

Specifies the name of the port.

Specify the name of your choice.

Possible values:

Alphanumeric ASCII character string with 0..32 characters

Auto-shutdown power

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

Possible values:

marked

unmarked (default setting)

Disable power at [hh:mm]

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

Possible values:

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

Re-enable power at [hh:mm]

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

Possible values:

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

1.10 Restart

[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 . 59:31:23 (default setting: 00:00:00)

Hour:Minute:Second

When the delay time elapses, the device restarts and goes through the following phases:

- If you activate the function in the [Diagnostics > System > Selftest](#) dialog, then the device performs the RAM self-test.
- The device starts the device software that the [Stored version](#) field displays in the [Basic Settings > Software](#) dialog.
- The device loads the settings from the "Selected" configuration profile. See the [Basic Settings > Load/Save](#) dialog.

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

Restart in

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

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

Cancel

Aborts a delayed restart.

Buttons

Clear FDB

Removes the MAC addresses from the forwarding table that have in the [Switching > Filter for MAC Addresses](#) dialog the value [Learned](#) in the [Status](#) column.

Clear ARP table

Removes the dynamically set up addresses from the ARP table.

See the [Diagnostics > System > ARP](#) dialog.

Clear port statistics

Resets the counter for the port statistics to 0.

See the [Basic Settings > Port](#) dialog, [Statistics](#) tab.

Clear management access statistics

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

See the [Diagnostics > System > System Information](#) dialog, [Used Management Ports](#) table.

Clear IGMP snooping data

Removes the IGMP Snooping entries and resets the counter in the [Information](#) frame to 0.

See the [Switching > IGMP Snooping > Global](#) dialog.

Clear log file

Removes the logged events from the log file.

See the [Diagnostics > Report > System Log](#) dialog.

Clear persistent log file

Removes the log files from the external memory.

See the [Diagnostics > Report > Persistent Logging](#) dialog.

Clear email notification statistics

Resets the counters in the [Information](#) frame to 0.

See the [Diagnostics > Email Notification > Global](#) dialog.

2 Time

The menu contains the following dialogs:

- [Basic Settings](#)
- [SNTP](#)

2.1 Basic Settings

[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:

- [\[Global\]](#)
- [\[Daylight saving time\]](#)

[Global]

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

Configuration

System time (UTC)

Displays the date and time in Universal Time Coordinated (UTC) format.

Set time from PC

The device takes over the time from your computer as the system time.

System time

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

Time source

Displays the time source from which the device 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.

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)

22 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.

not Synchronized

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 not 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 rcv 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

Hostname

Destination UDP port

Specifies the UDP port on which the external NTP or SNTP server listens for requests.

Possible values:

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

Exception: Port 2222 is reserved for internal functions.

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.

serverUnsyncronized

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.

not Synchronized

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.

syncToReferenceClock

The SNTP server is operating.
The local system clock is in sync with an external reference time source.

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)
- Exception: Port 2222 is reserved for internal functions.

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)
- Exception: Port 2222 is reserved for internal functions.

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, 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.

3 Device Security

The menu contains the following dialogs:

- [User Management](#)
- [Authentication List](#)
- [LDAP](#)
- [Management Access](#)
- [Pre-login Banner](#)
- [SSH Known Hosts](#)

3.1 User Management

[Device Security > User Management]

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

In this dialog, you manage the users of the local user management. You also specify the following settings here:

- Settings for the login
- Settings for saving the passwords
- Specify policy for valid passwords

The methods that the device uses for the authentication you specify in the [Device Security > Authentication List](#) dialog.

Configuration

This frame lets you specify settings for the login.

Login attempts

Specifies the number of 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 consecutive 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 [admini strator](#) 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)

Password policy

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

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

Upper-case characters (min.)

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

Possible values:

0 . 16 (default setting: 1)

The value 0 deactivates this setting.

Lower-case characters (min.)

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

Possible values:

0 . 16 (default setting: 1)

The value 0 deactivates this setting.

Digits (min.)

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

Possible values:

0 . 16 (default setting: 1)

The value 0 deactivates this setting.

Special characters (min.)

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

Possible values:

0 . 16 (default setting: 1)

The value 0 deactivates this setting.

Table

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

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

Buttons



Add

Opens the [Create](#) window to add a table row.

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




Remove

Removes the selected table row.

User name

Displays the name of the user account.

To 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 [admini str ator](#), 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.

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

When you specify the password for the first time, the device uses the same password in the [SNMP auth password](#) and [SNMP encryption password](#) columns.

- The device lets you specify different passwords in the [SNMP auth password](#) and [SNMP encryption password](#) columns.
- If you change the password in the current column, then the device also changes the passwords for the [SNMP auth password](#) and [SNMP encryption password](#) columns, but only if they are not individually specified previously.

Possible values:

Alphanumeric ASCII character string with 6..64 characters

The device accepts the following characters:

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

The minimum length of the password is specified in the [Configuration](#) frame. The device differentiates between upper and lower case.

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

The device constantly checks the minimum length of the password, even if the checkbox in the [Policy check](#) column is **unmarked**.

Role

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

Possible values:

[unauthorized](#)

The user is blocked, and the device rejects the user login 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.

Policy check

Activates/deactivates the password check.

Possible values:

[marked](#)

The password check is activated.

When you set up or change the password, the device checks the password according to the policy specified in the [Password policy](#) frame.

[unmarked](#) (default setting)

The password check is deactivated.

SNMP auth type

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

Possible values:

[hmacmd5](#) (default setting)

For this user account, the device uses protocol HMACMD5.

[hmacsha](#)

For this user account, the device uses protocol HMACSHA.

SNMP auth password

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

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

By default, the device uses the same password that you specify in the [Password](#) column.

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

Possible values:

Alphanumeric ASCII character string with 6..64 characters

The device accepts the following characters:

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

SNMP encryption type

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

Possible values:

[none](#)

No encryption.

[des](#) (default setting)

DES encryption

[aesCfb128](#)

AES128 encryption

SNMP encryption password

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

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

By default, the device uses the same password that you specify in the [Password](#) column.

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

Possible values:

Alphanumeric ASCII character string with 6..64 characters

The device accepts the following characters:

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

3.2 Authentication List

[Device Security > Authentication List]

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

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

- User management of the device
- LDAP
- RADIUS

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

- RADIUS
- IAS (Integrated Authentication Server)

In the default setting the following authentication lists are available:

- defaultDot1x8021AuthList
- defaultLogi nAuthList
- defaultV24AuthList

Table

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

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- In the [Name](#) field, you specify the name of the list.
Possible values:
Alphanumeric ASCII character string with 1..32 characters



Remove

Removes the selected table row.



Allocate applications

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

Click and select an 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 *Web interface*, 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 policies.
- If the first policy in the authentication list is *local* and the device denies the login credentials of the user, then it attempts to log the user into the device management using the other policies in the order specified.
- If the first policy in the authentication list is *radius* or *ldap* and the device rejects a login, then the login is immediately rejected without attempting to log in the user using another policy. If there is no response from the RADIUS or LDAP server, then the device attempts to authenticate the user with the next policy.

- If the first policy in the authentication list is [reject](#), then the devices immediately rejects the user login without attempting another policy.
- Verify that the authentication list [defaultV24AuthList](#) contains at least one policy different from [reject](#).

[ias](#)

The device authenticates the end devices logging in using 802.1X with the integrated authentication server (IAS). The integrated authentication server manages the login data in a separate database. See the [Network Security > 802.1X > IAS](#) dialog.


You can only assign this value to the authentication list [defaultDot1x8021AuthList](#).

[ldap](#)

The device authenticates the users with authentication data and access role saved in a central location. You specify the Active Directory server that the device uses in the [Device Security > LDAP > Configuration](#) dialog.

Dedicated applications

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

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

Active

Activates/deactivates the list.

Possible values:

[marked](#) (default setting)

The list is activated. The device uses the policies in this list when users access the device with the relevant application.

[unmarked](#)

The list is deactivated.

3.3 LDAP

[Device Security > LDAP]

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

The device forwards the login data of the user to the authentication server using the Lightweight Directory Access Protocol (LDAP). The authentication server decides if the login data is valid and transfers the authorizations of the user to the device.

Upon successful login, the device caches the login data. This speeds up the login process when users log into the device management again. In this case, no complex LDAP search operation is necessary.

The menu contains the following dialogs:

- [LDAP Configuration](#)
- [LDAP Role Mapping](#)

3.3.1 LDAP Configuration

[Device Security > LDAP > Configuration]

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

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

Operation

Operation

Enables/disables the *LDAP* client.

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

Possible values:

On

The *LDAP* client is enabled.

Off (default setting)

The *LDAP* client is disabled.

Configuration

Buttons



Flush cache

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

Client cache timeout [min]

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

Possible values:

1..1440 (default setting: 10)

Bind user

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

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

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

Possible values:

Alphanumeric ASCII character string with 0..64 characters

Bind user password

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

Possible values:

Alphanumeric ASCII character string with 0..64 characters

Base DN

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

Possible values:

Alphanumeric ASCII character string with 0..255 characters

User name attribute

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

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

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

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

Possible values:

Alphanumeric ASCII character string with 0..64 characters
(default setting: *userPrincipalName*)

Default domain

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

Possible values:

Alphanumeric ASCII character string with 0..64 characters

Certificates/CRLs

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

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

Buttons

 Clear all Certificates/CRLs

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


URL

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

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

- X.509 format
- . PEMfile name extension
- Base64-coded and enclosed by the lines
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
or
-----BEGIN CRL-----
...
-----END CRL-----

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

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

Start

Transfers the file specified in the [URL](#) field onto the device.

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

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

Table

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

Buttons



Add

Adds a table row.



Remove

Removes the selected table row.

Index

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

Description

Specifies the description.

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

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Address

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

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

Possible values:

Valid IPv4 address (default setting: 0.0.0.0)

Valid IPv6 address

DNS name in the format <domain>. <tl d> or <host>. <domain>. <tl d>

The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.

To establish an encrypted connection using a digital certificate, verify that the *Common Name* or *Subject Alternative Name* information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

_ldap._tcp.<domain>.<tl d>

Using this DNS name, the device queries the LDAP server list (SRV Resource Record) from the DNS server.

Destination TCP port

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

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

Possible values:

0..65535 (2¹⁶ - 1) (default setting: 389)

Exception: Port 2222 is reserved for internal functions.

Frequently used TCP-Ports:

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

Connection security

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

Possible values:

none

No encryption.

The device establishes an LDAP connection to the server and transmits the communication including the passwords in clear text.

[ssl](#)

Encryption with SSL.

The device establishes a TLS connection to the server and tunnels the LDAP communication over it.

[startTLS](#) (default setting)

Encryption with startTLS extension.

The device establishes an LDAP connection to the server and encrypts the communication.

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

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

Server status

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

Possible values:

[ok](#)

The server is reachable.

If in the [Connection security](#) column a value other than [none](#) is specified, then the device has verified the digital certificate of the server.

[unreachabl e](#)

Server is unreachable.

[other](#)

The device has not established a connection to the server yet.

Active

Activates/deactivates the use of the server.

Possible values:

[marked](#)

The device uses the server.

[unmarked](#) (default setting)

The device does not use the server.

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

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

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

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

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

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

On this basis, the device checks any mapping.

- Does the user object contain the required attribute?
or
- Is the user member of the group?

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

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

Configuration

Matching policy

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

Possible values:

highest (default setting)

The device applies the access role with more extensive authorizations.

first

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

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- In the [Index](#) field, you specify the index number.

Possible values:

1 . 64



Remove

Removes the selected table row.

Index

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

Role

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

Possible values:

[unauthorized](#) (default setting)

The user is blocked, and the device rejects the user login.

Assign this value to temporarily lock the user account. If an error is detected when another role is being assigned, then the device assigns this access role to the user account.

[guest](#)

The user is authorized to monitor the device.

[auditor](#)

The user is authorized to monitor the device and to save the log file in the [Diagnostics > Report > Audit Trail](#) dialog.

[operator](#)

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

[administrator](#)

The user is authorized to monitor the device and to change the settings.

Type

Specifies if a group or an attribute with an attribute value is specified in the [Parameter](#) column.

Possible values:

[attribute](#) (default setting)

The [Parameter](#) column contains an attribute with an attribute value.

[group](#)

The [Parameter](#) column contains the “Distinguished Name” (DN) of a group.

Parameter

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

Possible values:

Alphanumeric ASCII character string with 0..255 characters

The device differentiates between upper and lower case.

- If in the *Type* column the value *attribute* is specified, then you specify the attribute in the form of *Attribute_name=Attribute_value*.

Example: *l=Germany*

- If in the *Type* column the value *group* is specified, then you specify the “Distinguished Name” (DN) of a group.

Example: *CN=admi n- users, OU=Groups, DC=exampl e, DC=com*

Active

Activates/deactivates the role mapping.

Possible values:

marked

The role mapping is active.

unmarked (default setting)

The role mapping is inactive.

3.4 Management Access

[Device Security > Management Access]

The menu contains the following dialogs:

- [Server](#)
- [IP Access Restriction](#)
- [Web](#)
- [Command Line Interface](#)
- [SNMPv1/v2 Community](#)

3.4.1 Server

[Device Security > Management Access > Server]

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

The dialog contains the following tabs:

- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

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

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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.
- You activate/deactivate the write access for the *read and write* authorization in the [Device Security > Management Access > SNMPv1/v2 Community](#) dialog.

unmarked (default setting)

SNMP version 1 access is inactive.

SNMPv2

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

Possible values:

marked

SNMP version 2 access is active.

- You specify the community names in the [Device Security > Management Access > SNMPv1/v2 Community](#) dialog.
- You activate/deactivate the write access for the *read and write* authorization in the [Device Security > Management Access > SNMPv1/v2 Community](#) dialog.

unmarked (default setting)

SNMP version 2 access is inactive.

SNMPv3

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

Possible values:

marked (default setting)

Access is activated.

unmarked

Access is deactivated.

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

UDP port

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

Possible values:


1.. 65535 (2¹⁶ - 1) (default setting: 161)

Exception: Port 2222 is reserved for internal functions.

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

Click the  button.

Select in the *Basic Settings > Load/Save* dialog the active configuration profile.

Click the  button to save the current settings.

Restart the device.

SNMPover802

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

Possible values:

marked

Access is activated.

unmarked (default setting)

Access is deactivated.

[Telnet]

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

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

Operation

Telnet server

Enables/disables the Telnet server.

Possible values:

On

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 the access to the Command Line Interface is only possible through the serial interface of the device.

Configuration

TCP port

Specifies the number of the TCP port on which the device receives 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 private and public keys (host keys) required for RSA directly in the device. As an alternative, transfer your own host key in PEM format onto the device.

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

Operation

SSH server

Enables/disables the SSH server.

Possible values:

On (default setting)

The SSH server is enabled.

The access to the device management is possible through the Command Line Interface using an encrypted SSH connection.

You can start the server only if there is an RSA signature in the device.

Off

The SSH server is disabled.

When you disable the SSH server, the existing connections remain established. However, the device helps prevent new connections from being set up.

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

Configuration

TCP port

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

Possible values:

1.. 65535 ($2^1 - 1$) (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

A key is present.

unmarked

No key is present.

Create

Generates a host key in the device. The prerequisite is that the [SSH](#) server is disabled.

Length of the key generated:

- 2048 bit (RSA)

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

As an alternative, transfer your own host key in PEM format onto the device. See the [Key import](#) frame.

Delete

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

Oper status

Displays if the device currently generates a host key.

It is possible that another user triggered this action.

Possible values:

[rsa](#)

The device currently generates an RSA host key.

[none](#)

The device does not generate a host key.

Fingerprint

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

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

Fingerprint type

Specifies which fingerprint the *RSA fingerprint* field displays.

Possible values:

[md5](#)



The *RSA fingerprint* field displays the fingerprint as hexadecimal MD5 hash.

[sha256](#) (default setting)

The *RSA fingerprint* field displays the fingerprint as Base64-coded SHA256 hash.

RSA fingerprint

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

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

Key import

URL


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

The device accepts the RSA key if it has the following key length:

- 2048 bit (RSA)

The device gives you the following options for 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 from an FTP server

This option is not recommended 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 from a TFTP server
This option is not recommended 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 from an SCP or SFTP server
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.

As an alternative, transfer your own 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.

[del ete](#)

The device currently deletes a digital certificate.

[gener ate](#)

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 SHA1 fingerprint of the digital certificate.

[sha256](#) (default setting)

The *Fingerprint* field displays the SHA256 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
- . PEMfile name extension

- Base64-coded and enclosed by the lines
 - -----BEGIN PRIVATE KEY-----
 - ...
 - END PRIVATE KEY-----
 - or
 - -----BEGIN CERTIFICATE-----
 - ...
 - END CERTIFICATE-----
- RSA key with 2048 bit length

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 from an FTP server

This option is not recommended 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 from a TFTP server

This option is not recommended 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 from an SCP or SFTP server

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://<user>:<password>@<IP address>[: port]/<path>/<file name>`

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

Start

Transfers the file specified in the [URL](#) field onto the device.

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

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

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

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

Operation

Operation

Enables/disables the *IP Access Restriction* function.

Possible values:

On

The *IP Access Restriction* function is enabled.

The access to the device management is restricted.

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

Off (default setting)

The *IP Access Restriction* function is disabled.

Table

You have the option of defining up to 16 table rows and activating them separately.

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

IEC61850-MMS

Activates/deactivates the access to the MMS server.

Possible values:

`marked` (default setting)

IEC61850-MMS access is active. Access is possible from the adjacent IP address range.

`unmarked`

IEC61850-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.

Active

Activates/deactivates the table row.

Possible values:

`marked` (default setting)

The table row is active. The device restricts the access to the device management from the specified IP address range for the selected applications.

`unmarked`

The table row is inactive. The device does not restrict access to the device management from the specified IP address range for the selected applications.

3.4.3 Web

[Device Security > Management Access > Web]

In this dialog, you specify settings for the Graphical User Interface.

Configuration

Web interface session timeout [min]

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

Possible values:

0 . 160 (default setting: 5)

The value 0 deactivates the function, and the user remains logged in when inactive.

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

In this dialog, you specify settings for the Command Line Interface. For further information about the Command Line Interface, see the “Command Line Interface” reference manual.

The dialog contains the following tabs:

- [\[Global\]](#)
- [\[Login banner\]](#)

[Global]

This tab lets you change the prompt in the Command Line Interface and specify the automatic closing of sessions through the serial interface when they have been inactive.

The device has the following serial interfaces.

- USB-C interface

Configuration

Login prompt

Specifies the character string that the device displays in the Command Line Interface at the start of every command line.

Possible values:

Alphanumeric ASCII character string with 0..128 characters
(0x20..0x7E) including space characters

Wildcards

- %d date
- %i IP address
- %m MAC address
- %p product name
- %t time

Default setting: (GRS)

Changes to this setting are immediately effective in the active Command Line Interface session.

Serial interface timeout [min]

Specifies the time in minutes after which the device automatically closes the session of an inactive user logged into the device management with the Command Line Interface through the serial interface.

Possible values:

0..160 (default setting: 5)

The value 0 deactivates the function, and the user remains logged 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>

<Li ne break>

3.4.5 SNMPv1/v2 Community

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

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

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

You activate the access to the device using SNMPv1/v2 in the [Device Security > Management Access > Server](#) dialog.

Table

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

If the [SNMP V1/V2 readOnly](#) checkbox is marked, then the application receives *read-only* authorization.

Read

For requests with the community name entered, the application receives *read-only* authorization.

Name

Specifies the community name for the adjacent authorization.

Possible values:

Alphanumeric ASCII character string with 0..64 characters

The device accepts the following characters:

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

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

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

Configuration

SNMP V1/V2 readOnly

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

Possible values:

marked

The write access for the **Write** community is inactive.

For requests with the community name entered, the application receives *read-only* authorization.

unmarked (default setting)

The write access for the **Write** community is active.

For requests with the community name entered, the application receives *read and write* authorization.

3.5 Pre-login Banner

[Device Security > Pre-login Banner]

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

The users see this text in the login dialog of the Graphical User Interface and of the Command Line Interface. Users logging into the device management with SSH see the text - regardless of the client used - before or during the login.

To display the text only in the Command Line Interface, use the settings in the [Device Security > Management Access > CLI](#) dialog.

Operation

Operation

Enables/disables the [Pre-login Banner](#) function.

Using the [Pre-login Banner](#) function, the device displays a greeting or information text in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

On

The [Pre-login Banner](#) function is enabled.

The device displays the text specified in the [Banner text](#) field in the login dialog.

Off (default setting)

The [Pre-login Banner](#) function is disabled.

The device does not display a text in the login dialog. When you enter a text in the [Banner text](#) field, the device saves this text.

Banner text

Banner text

Specifies information text that the device displays in the login dialog of the Graphical User Interface and of the Command Line Interface.

Possible values:

Alphanumeric ASCII character string with 0..512 characters
([0x20](#) . [0x7E](#)) including space characters

[<Tab>](#)

[<Line break>](#)

3.6 SSH Known Hosts

[Device Security > SSH Known Hosts]

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

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

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

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

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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. This option is not recommended if you transmit data over untrusted networks.

Possible values:

- Base64-coded SHA256 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 SHA256 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.



Collapses the levels. The overview then displays only the first level of the items.



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



Expands the current item and displays the items of the next lower level.




Collapses the item and hides the items of the underlying levels.

4.2 Port Security

[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



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 134](#).

Port

Displays the port number.

Active

Activates/deactivates the *Port Security* function on the port.

Possible values:

marked

The device checks every data packet received on the port and forwards it only if the source address of the data packet is desired. Also enable the *Port Security* function in the *Operation* frame.

unmarked (default setting)

The device forwards every data packet received on the port without checking the source address.

Note: When you operate the device as an active participant within an *MRP* ring, we recommend that you unmark the checkbox for the ring ports.

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

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Port Security* on the port.

Possible values:

marked (default setting)

The *Auto-Disable* function is active on the port.

The device disables the port and optionally sends an SNMP trap when one of the following events occurs:

- The device registers at least one address of a sender that is not desired on the port.
- The device registers more addresses than specified in the *Dynamic limit* column.

The *Link status* LED for the port flashes 3 x per period. This restriction makes *MAC Spoofing* attacks more difficult.

The prerequisite is that in the *Configuration* frame the *Auto-disable* checkbox is marked.

- The *Diagnostics > Ports > Auto-Disable* dialog displays which ports are currently disabled due to the parameters being exceeded.
- After a waiting period, the *Auto-Disable* function enables the port again automatically. For this you go to the *Diagnostics > Ports > Auto-Disable* dialog and specify a waiting period for the relevant port in the *Reset timer [s]* column.

unmarked

The *Auto-Disable* function is inactive on the port.

Send trap

Activates/deactivates the sending of SNMP traps when the device discards a data packet from an undesired sender on the port.

Possible values:

marked

The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.

If the device discards data packets from a sender that is not desired on the port, then the device sends an SNMP trap.

unmarked (default setting)

The sending of SNMP traps is inactive.

Trap interval [s]

Specifies the delay time in seconds that the device waits after sending an SNMP trap before sending the next SNMP trap.

Possible values:

0 . 3600 (default setting: 0)

The value 0 deactivates the delay time.

Dynamic limit

Specifies the upper limit for the number of automatically registered addresses (*dynamic entries*). When the upper limit is reached, the device stops “learning” on this port.

Adjust the value to the number of expected senders.

If the port registers more addresses than specified here, then the *Auto-Disable* function disables the port. The prerequisite is that you mark the checkbox in the *Auto-disable* column and the *Auto-disable* checkbox in the *Configuration* frame.

Possible values:

- 0
No automatic registering of addresses on this port.
- 1..600 (default setting: 600)

Static limit

Specifies the upper limit for the number of addresses associated with the port using the *Wizard* window (*static entries*).

Possible values:

- 0
No association possible between the port and a desired sender. Only specify this value if you specify a value > 0 in the *Dynamic limit* column.
- 1..64 (default setting: 64)

Dynamic entries

Displays the number of addresses that the device has automatically registered.

Static MAC entries

Displays the number of MAC addresses associated with the port.

Last violating VLAN ID/MAC

Displays the VLAN ID and MAC address of an undesired sender whose data packets the device last discarded on this port.

Sent traps

Displays the number of discarded data packets on this port that caused the device to send an SNMP trap.


[Wizard: Port security]

The *Wizard* window helps you associate the ports with the address of one or more desired senders.

The *Wizard* window guides you through the following steps:

- [Select port](#)
- [MAC addresses](#)

Note: The device saves the addresses associated with the port until you deactivate the *Port Security* function on the relevant port or disable the *Port Security* function in the device.

After closing the *Wizard* window, click the  button to save your settings.

Select port

Port

Specifies the port that you associate with the address of desired senders in the next step.

MAC addresses

Static entries (x/y)

Displays the number of addresses associated with the port using the *Wizard* window and the upper limit for *static entries*. The lower part of the *Wizard* window displays the entries in detail, if any.



Removes the entries in the lower part of the *Wizard* window. The device removes the respective association between a port and the desired senders.

VLAN ID

Specifies the VLAN ID of the desired sender.

Possible values:

1..4042

MAC address

Specifies the MAC address of the desired sender.

Possible values:

Valid Unicast MAC address

Specify the value with a colon separator, for example 00:11:22:33:44:55.

Note: You can assign a MAC address to only one port.

Add

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 [radi us](#) policy to the [8021x](#) list.

To authenticate the end devices through the Integrated Authentication Server (IAS) you assign the [i as](#) 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



Removes the selected table row.

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



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.

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.

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



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.



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)

Exception: Port 2222 is reserved for internal functions.

Secret

Displays ***** (asterisks) when you specify a password with which the device logs into the server. To change the password, click the relevant field.

Possible values:

Alphanumeric ASCII character string with 1..64 characters

You get the password from the administrator of the authentication server.

Primary server

Specifies the authentication server as primary or secondary.

Possible values:

marked

The server is specified as the primary authentication server. The device sends the login data for authenticating the users to this authentication server.

This setting applies only if more than one server in the table has the same value in the *Name* column.

unmarked (default setting)

The server is the secondary authentication server. When the device does not receive a response from the primary authentication server, the device sends the login data to the secondary authentication server.

Active

Activates/deactivates the connection to the server.

The device uses the server, if you specify in the *Device Security > Authentication List* dialog the value *radius* in one of the columns *Policy 1* to *Policy 5*.

Possible values:

marked (default setting)

The connection is active. The device sends the login data for authenticating the users to this server if the preconditions named above are fulfilled.

unmarked

The connection is inactive. The device does not send any login data to this server.

4.4.3 RADIUS Accounting Server

[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.



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)

Exception: Port 2222 is reserved for internal functions.

Secret

Displays ***** (asterisks) when you specify a password with which the device logs into the server. To change the password, click the relevant field.

Possible values:

Alphanumeric ASCII character string with 1..16 characters

You get the password from the administrator of the authentication server.

Active

Activates/deactivates the connection to the server.

Possible values:

marked (default setting)

The connection is active. The device sends traffic data to this server if the preconditions named above are fulfilled.

unmarked

The connection is inactive. The device does not send any traffic data to this server.

4.4.4 RADIUS Authentication Statistics

[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.

The device supports the detection of the following scan types:

- Null scans
- Xmas scans
- SYN/FIN scans
- TCP Offset attacks
- TCP SYN attacks
- L4 Port attacks
- Minimal Header scans

Null Scan filter

Activates/deactivates the Null Scan filter.

The device detects and discards incoming TCP packets with the following properties:

- No TCP flags are set.
- The TCP sequence number is 0.

Possible values:

`marked`

The filter is active.

`unmarked` (default setting)

The filter is inactive.

Xmas filter

Activates/deactivates the Xmas filter.

The device detects and discards incoming TCP packets with the following properties:

- The TCP flags *FIN*, *URG* and *PSH* are simultaneously set.
- The TCP sequence number is 0.

Possible values:

`marked`

The filter is active.

`unmarked` (default setting)

The filter is inactive.

SYN/FIN filter

Activates/deactivates the SYN/FIN filter.

The device detects incoming data packets with the TCP flags *SYN* and *FIN* set simultaneously and discards them.

Possible values:

`marked`

The filter is active.

`unmarked` (default setting)

The filter is inactive.

TCP Offset protection

Activates/deactivates the TCP Offset protection.

The TCP Offset protection detects incoming TCP data packets whose fragment offset field of the IP header is equal to 1 and discards them.

The TCP Offset protection accepts UDP and ICMP packets whose fragment offset field of the IP header is equal to 1.

Possible values:

`marked`

The protection is active.

`unmarked` (default setting)

The protection is inactive.

TCP SYN protection

Activates/deactivates the TCP SYN protection.

The TCP SYN protection detects incoming data packets with the TCP flag *SYN* set and a L4 source port <1024 and discards them.

Possible values:

`marked`

The protection is active.

`unmarked` (default setting)

The protection is inactive.

L4 Port protection

Activates/deactivates the L4 Port protection.

The L4 Port protection detects incoming TCP and UDP data packets whose source port number and destination port number are identical and discards them.

Possible values:

`marked`

The protection is active.

`unmarked` (default setting)

The protection is inactive.

Min. Header Size filter

Activates/deactivates the Minimal Header filter.

The Minimal Header filter compares the TCP header of incoming data packets. If the data offset value multiplied by 4 is smaller than the minimum TCP header size, then the filter discards the data packet.

Possible values:

marked

The filter is active.

unmarked (default setting)

The filter is inactive.

Min. TCP header size

Displays the minimum size of a valid TCP header.

IP

Land Attack filter

Activates/deactivates the *Land Attack* filter. With the *Land Attack* method, the attacking station sends data packets whose source and destination addresses are identical to the IP address of the recipient.

Possible values:

marked

The filter is active. The device discards data packets whose source and destination addresses are identical.

unmarked (default setting)

The filter is inactive.

ICMP

This dialog provides you with filter options for the following ICMP parameters:

- Fragmented data packets
- ICMP packets from a specific size upwards

Fragmented packets filter

Activates/deactivates the filter for fragmented ICMP packets.

The filter detects fragmented ICMP packets and discards them.

Possible values:

marked

The filter is active.

unmarked (default setting)

The filter is inactive.

Packet size filter

Activates/deactivates the filter for incoming ICMP packets.

The filter detects ICMP packets whose payload size exceeds the size specified in the *Allowed payload size [byte]* field and discards them.

Possible values:

marked

The filter is active.

unmarked (default setting)

The filter is inactive.

Allowed payload size [byte]

Specifies the maximum allowed payload size of ICMP packets in bytes.

Mark the *Packet size filter* checkbox if you want the device to discard incoming data packets whose payload size exceeds the maximum allowed size for ICMP packets.

Possible values:

0 . 1472 (default setting: 512)

4.6 ACL

[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:

- **permi t**: 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 specify a new name. When you add a new name, click the **+** icon.
- In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first.



Remove

Removes the selected table row.

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.

Index

Displays the number of the rule within the Access Control List. You specify the index number when you add a table row.

If the Access Control List contains multiple rules, then the device processes the rule with the 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 specify a new name. When you add a new name, click the **+** icon.
- In the *Index* field, you specify the number of the rule within the Access Control List. If the Access Control List contains multiple rules, then the device processes the rule with the lowest index value first.



Remove

Removes the selected table row.

Group name

Displays the name of the Access Control List. The Access Control List contains the rules.

Index

Displays the number of the rule within the Access Control List. You specify the index number when you add a table row.

If the Access Control List contains multiple rules, then the device processes the rule with the numerically lowest value first.

Action

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

Possible values:

- [permi t](#) (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:

- [mar ked](#)
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.
- [unmar ked](#) (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 assignment of Access Control Lists to ports and VLANs results in the following different types of ACLs:

- Port-based IPv4 ACLs
- Port-based MAC ACLs
- VLAN-based IPv4 ACLs
- VLAN-based MAC ACLs

The device lets you apply the Access Control Lists to data packets received (*inbound*).

Note: Before you enable the function, verify that at least one active table row in the table lets you access. Otherwise, the connection to the device terminates if you change the settings. To access the device management is possible only using the CLI through the serial interface of the device.

Table

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

Buttons



Add

Opens the *Create* window to assign a rule to a port or a VLAN.

- 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 ($2^{32} - 1$)

Active

Displays if the Access Control List on the port or in the VLAN is active.

Possible values:

`marked` (default setting)

The Access Control List is active.

`unmarked`

The Access Control List is inactive.

5 Switching

The menu contains the following dialogs:

- [Switching Global](#)
- [Rate Limiter](#)
- [Filter for MAC Addresses](#)
- [IGMP Snooping](#)
- [MRP-IEEE](#)
- [GARP](#)
- [QoS/Priority](#)
- [VLAN](#)
- [L2-Redundancy](#)

5.1 Switching Global

[Switching > Global]

This dialog lets you specify the following settings:

- Change the Aging time of the MAC address table (forwarding database) entries
- Enable the flow control in the device
- Activate the [VLAN-unaware mode](#) function

If a large number of data packets are received in the priority queue of a port at the same time, then this can cause the port memory to overflow. This happens, for example, when the device receives data on a Gigabit port and forwards it to a port with a lower bandwidth. The device discards superfluous data packets.

The flow control mechanism defined in IEEE 802.3 helps ensure that no data packets are lost due to a buffer overflow on a port. Shortly before the buffer memory of a port is completely full, the device signals to the connected devices that it is not accepting any more data packets from them.

- In full-duplex mode, the device sends a pause data packet.
- 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.

According to IEEE 802.1Q, the device forwards data packets with a VLAN tag in a VLAN 1. However, a few applications on connected end devices send or receive data packets with a VLAN ID=0. Data packets with a VLAN ID=0 are called *Priority Tagged Frames*. When the device receives one of these data packets, before forwarding it, the device overwrites the original value in the data packet with the VLAN ID of the receiving port.

If you activate the [VLAN-unaware mode](#) function, then this deactivates the VLAN settings in the device. The device then transparently forwards the data packets and evaluates the priority information contained only in the data packet.

Configuration

MAC address

Displays the MAC address of the device.

Aging time [s]

Specifies the aging time in seconds.

Possible values:

`10 . 500000` (default setting: `30`)

The device monitors the age of the learned unicast MAC addresses. The device deletes address entries that exceed a particular age (aging time) from its MAC address table (forwarding database).

You find the MAC address table (forwarding database) in the [Switching > Filter for MAC Addresses](#) dialog.

Flow control

Activates/deactivates the flow control in the device.

Possible values:

`marked`

The flow control is active in the device.

Additionally activate the flow control on the required ports. See the [Basic Settings > Port](#) dialog, [Configuration](#) tab, checkbox in the [Flow control](#) column.

`unmarked` (default setting)

The flow control is inactive in the device.

If you are using a redundancy function, then 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.

VLAN-unaware mode

Activates/deactivates the mode in which the device ignores the VLAN ID and forwards the data packets unchanged. The device continues to evaluate the priority information in the data packets.

On the connected end devices, only some applications require receiving data packets with a VLAN ID=0. If applications in the network require this, then activate the function.

Possible values:

`marked`

The device operates in the *VLAN-unaware* mode according to IEEE 802.1Q:

- The device ignores the VLAN settings in the device and the VLAN ID in the data packets. The device forwards the data packets based on their destination MAC address.
- The device evaluates the priority information contained in the VLAN tag of the data packets.
- The device ignores the VLAN settings specified in the [Switching > VLAN > Configuration](#) and [Switching > VLAN > Port](#) dialogs.

Note: You specify the VLAN ID 1 for every function in the device which uses VLAN settings. Among other things, this applies to static filters, MRP and IGMP Snooping.

[unmarked](#) (default setting)

The device operates in the *VLAN-aware* mode according to IEEE 802.1Q:

- The device evaluates the VLAN tags in the data packets.
- The device forwards the data packets based on their destination MAC address or destination IP address in the corresponding VLAN.
- The device evaluates the priority information contained in the data packet.
- When the device receives a data packet with a VLAN ID=0 it assigns the VLAN ID of the port to the data packet. See the [Switching > VLAN > Port](#) dialog.

5.2 Rate Limiter

[Switching > Rate Limiter]

The device lets you limit the amount of data packets on the ports to help provide stable operation even with a large data volume. If the amount of data packets on a port exceed the threshold value, then the device discards the excess data packets on this port.

The rate limiter function operates only on Layer 2, and is used to limit the effects of storms of data packets that flood the device (typically Broadcasts).

The rate limiter function ignores protocol information on higher layers, such as IP or TCP.

The dialog contains the following tabs:

- [\[Ingress\]](#)
- [\[Egress\]](#)

[Ingress]

In this tab you enable the *Rate Limiter* function. The threshold value specifies the maximum amount of data packets the port receives. If the amount of data packets on a port exceed the specified threshold value, then the device discards the excess data packets on this port.

Table

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

Port

Displays the port number.

Threshold

Specifies the threshold value for broadcast, multicast, and unicast data packets on this port:

Possible values:

0 (default setting)

The *Rate Limiter* function is deactivated on this port.

1.. 24414 at 100 Mbit/s

1.. 244140 at 1000 Mbit/s

If the value *percent* is specified in the *Unit* column, then specify a percentage value between 1 and 100.

If the value *pps* is specified in the *Unit* column, then specify an absolute value.

The rate limiter function calculates the threshold value based on 512-byte-sized packets.

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

Unit

Specifies the unit for the threshold value:

Possible values:

`percent` (default setting)

Specifies the threshold value as a percentage of the data rate of the port.

`pps`

Specifies the threshold value in data packets per second.

Broadcast mode

Activates/deactivates the rate limiter function for received broadcast data packets.

Possible values:

`marked`

`unmarked` (default setting)

If the threshold value is exceeded, then the device discards the excess broadcast data packets on this port.

Multicast mode

Activates/deactivates the rate limiter function for received multicast data packets.

Possible values:

`marked`

`unmarked` (default setting)

If the threshold value is exceeded, then the device discards the excess multicast data packets on this port.

Unknown unicast mode

Activates/deactivates the rate limiter function for received unicast data packets with an unknown destination address.

Possible values:

`marked`

`unmarked` (default setting)

If the threshold value is exceeded, then the device discards the excess unicast data packets on this port.

[Egress]

In this tab you specify the egress transmission rate on the port.

Table

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

Port

Displays the port number.

Bandwidth [%]

Specifies the egress transmission rate.

Possible values:

0 (default setting)

The bandwidth limitation is disabled.

1..100

The bandwidth limitation is enabled.

This value specifies the percentage of overall link speed for the port in 1% increments.

5.3 Filter for MAC Addresses

[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

Removes the MAC addresses from the forwarding table that have the value [Learned](#) in the [Status](#) column.

Address

Displays the destination MAC address to which the table row 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:

Lear ned

Address filter set up automatically by the device based on received data packets.

Mgmt

MAC address of the device. The address filter is protected against changes.

Other

Static address added by the following function:

– *802.1X*

– *Port Security*

Permanent

Address filter set up manually. The address filter stays set up permanently.

GMRP

Multicast address filter automatically set up by GMRP.

IGMP

Address filter automatically set up by IGMP Snooping.

MRP-MMRP

Multicast address filter automatically set up by MMRP.

<Port number>

Displays how the corresponding port transmits data packets which it directs to the adjacent destination address.

Possible values:

–

The port does not transmit any data packets to the destination address.

Lear ned

The port transmits data packets to the destination address. The device has automatically set up the filter based on received data packets.

IGMP Lear ned

The port transmits data packets to the destination address. The device has automatically set up the filter based on IGMP.

uni cast stati c

The port transmits data packets to the destination address. A user has set up the filter.

mul ti cast stati c

The port transmits data packets to the destination address. A user 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

Removes 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 ($2^{31} - 1$)

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)

[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 193](#).

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.

A = Automatic

The device detected the port as a query port. The prerequisite is that you set up the port as [Learn by LLDP](#).

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.

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.

[Send to query ports](#)

The device forwards data packets with an unknown MAC Multicast address to the query ports.

Table

In the table you specify the settings for known Multicasts for the set-up VLANs.

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 MRP-IEEE

[Switching > MRP-IEEE]

The IEEE 802.1ak amendment to the IEEE 802.1Q standard introduced the Multiple Registration Protocol (MRP) to replace the Generic Attribute Registration Protocol (GARP). The IEEE standards association also modified and replaced the GARP applications, GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP). The Multiple MAC Registration Protocol (MMRP) and the Multiple VLAN Registration Protocol (MVRP) replace these protocols.

MRP-IEEE helps confine traffic to the required areas of the LAN. To confine traffic, the MRP-IEEE applications distribute attribute values to participating MRP-IEEE devices across a LAN registering and de-registering multicast group membership and VLAN identifiers.

Registering group participants lets you reserve resources for specific data packets transversing a LAN. Defining resource requirements regulates the level of traffic, allowing the devices to determine the required resources and provides for dynamic maintenance of the allocated resources.

The menu contains the following dialogs:

- [MRP-IEEE Configuration](#)
- [MRP-IEEE Multiple MAC Registration Protocol](#)
- [MRP-IEEE Multiple VLAN Registration Protocol](#)

5.5.1 MRP-IEEE Configuration

[Switching > MRP-IEEE > Configuration]

This dialog lets you set the various MRP timers. By maintaining a relationship between the various timer values, the protocol operates efficiently and with less likelihood of unnecessary attribute withdraws and re-registrations. The default timer values effectively maintain these relationships.

When you reconfigure the timers, maintain the following relationships:

- To allow for re-registration after a Leave or LeaveAll event, even if there is a lost message, specify the LeaveTime to: $(2 \times \text{JoinTime}) + 60$.
- To minimize the volume of rejoining data packets generated following a LeaveAll event, specify the value for the LeaveAll timer larger than the LeaveTime value.

Table

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

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 transiting to the empty (MT) state.

Possible values:

20 . 600 (default setting: 60)

Leave all time [1/100s]

Specifies the LeaveAll timer which controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs.

Possible values:

200 . 6000 (default setting: 1000)

5.5.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

The Multiple MAC Registration Protocol (MMRP) lets end devices and MAC switches register and de-register group membership and individual MAC address information with switches located in the same LAN. The switches within the LAN disseminate the information through switches that support extended filtering services. Using the MAC address information, MMRP lets you confine multicast traffic to the required areas of a Layer 2 network.

For an example of how MMRP works, consider a security camera mounted on a mast overlooking a building. The camera sends multicast packets onto a LAN. You have 2 end devices installed for surveillance in separate locations. You register the MAC addresses of the camera and the 2 end devices in the same multicast group. You then specify the MMRP settings on the ports to send the multicast group packets to the 2 end devices.

The dialog contains the following tabs:

- [\[Configuration \]](#)
- [\[Service requirement \]](#)
- [\[Statistics \]](#)

[Configuration]

In this tab you select active MMRP port participants and set the device to transmit periodic events. The dialog also lets you enable VLAN registered MAC address broadcasting.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the devices associated with the active port.

Operation

Operation

Enables/disables the global *MMRP* function in the device. The device participates in MMRP message exchanges.

Possible values:

On

The device is a normal participant in MMRP message exchanges.

Off (default setting)

The device ignores MMRP messages.

Configuration

Periodic state machine

Enables/disables the global periodic state machine in the device.

Possible values:

On

With MMRP *Operation* enabled globally, the device transmits MMRP messages in one-second intervals, on MMRP participating ports.

Off (default setting)

Disables the periodic state machine in the device.

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 [Forward All](#) 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 [Forward All](#) 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 [Forward All](#) ports.

[F](#)

Specifies the [Forbidden](#) traffic setting on the port. The device blocks dynamic MMRP [Forward All](#) service requirements. With [Forward All](#) 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 (MMRPDU) 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.

5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

The Multiple VLAN Registration Protocol (MVRP) provides a mechanism that lets you distribute VLAN information and configure VLANs dynamically. For example, when you configure a VLAN on an active MVRP port, the device distributes the VLAN information to other MVRP enabled devices. Using the information received, an MVRP enabled device dynamically generates the VLAN trunks on other MVRP enabled devices as needed.

The dialog contains the following tabs:

- [\[Configuration\]](#)
- [\[Statistics\]](#)

[Configuration]

In this tab you select active MVRP port participants and set the device to transmit periodic events.

A periodic state machine exists for each port and transmits periodic events regularly to the applicant state machines associated with active ports. Periodic events contain information indicating the status of the VLANs associated with the active port. Using the periodic events, MVRP enabled switches dynamically maintain the VLANs.

Operation

Operation

Enables/disables the global Applicant Administrative Control which specifies if the Applicant state machine participates in MMRP message exchanges.

Possible values:

On

Normal Participant. The Applicant state machine participates in MMRP message exchanges.

Off (default setting)

Non-Participant. The Applicant state machine ignores MMRP messages.

Configuration

Periodic state machine

Enables/disables the periodic state machine in the device.

Possible values:

On

The periodic state machine is enabled.

With MVRP *Operation* enabled globally, the device transmits MVRP periodic events every 1 s, on MVRP participating ports.

Off (default setting)

The periodic state machine is disabled.

Disables the periodic state machine in the device.

Table

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

5.6 GARP

[Switching > GARP]

The Generic Attribute Registration Protocol (GARP) is defined by the IEEE standards association to provide a generic framework so switches can register and deregister attribute values, such as VLAN identifiers and multicast group membership.

When an attribute for a participant is registered or deregistered according to GARP, the participant is modified according to specific rules. The participants are a set of reachable end stations and network devices. The defined set of participants at any given time, along with their attributes, is the reachability tree for the subset of the network topology. The device forwards the data frames only to the registered end stations. The station registration helps prevent attempts to send data to the end stations that are unreachable.

Note: Before you enable the *GMRP* function, verify that the *MMRP* function is disabled.

The menu contains the following dialogs:

- *GMRP*
- *GVRP*

5.6.1 GMRP

[Switching > GARP > GMRP]

The GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) that provides a mechanism allowing network devices and end stations to dynamically register group membership. The devices register group membership information with the devices attached to the same LAN segment. GARP also lets the devices distribute the information across the network devices that support extended filtering services.

GMRP and GARP are industry-standard protocols defined by the IEEE 802.1D.

Operation

Operation

Enables/disables the global [GMRP](#) function in the device. The device participates in GMRP message exchanges.

Possible values:

[On](#)

GMRP is enabled.

[Off](#) (default setting)

The device ignores GMRP messages.

Multicasts

Unknown multicasts

Enables/disables the unknown multicast data to be either flooded or discarded.

Possible values:

[disc](#)

The device discards unknown multicast data.

[flood](#) (default setting)

The device forwards unknown multicast data to every port.

Table

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

Port

Displays the port number.

GMRP active

Activates/deactivates the port *GMRP* participation.

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

Possible values:

marked (default setting)

The port *GMRP* participation is active.

unmarked

The port *GMRP* participation is inactive.

Service requirement

Specifies the ports on which multicast forwarding applies.

Possible values:

Forward all unregistered groups (default setting)

The device forwards data destined to *GMRP*-registered multicast MAC addresses on the VLAN.

The device forwards data to the unregistered groups.

Forward all groups

The device forwards data destined to every group, registered or unregistered.

5.6.2 GVRP

[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.

5.7 QoS/Priority

[Switching > QoS/Priority]

Communication networks transmit a number of applications at the same time that have different requirements as regards availability, bandwidth and latency periods.

QoS (Quality of Service) is a procedure defined in IEEE 802.1D. It is used to distribute resources in the network. You therefore have the possibility of providing minimum bandwidth for necessary applications. The prerequisite is that the end devices and the devices in the network support prioritized data transmission. Data packets with high priority are given preference when transmitted by devices in the network. You transfer data packets with lower priority when there are no data packets with a higher priority to be transmitted.

The device provides the following setting options:

- You specify how the device evaluates QoS/prioritization information for inbound data packets.
- For outbound packets, you specify which QoS/prioritization information the device writes in the data packet (for example priority for management packets, *Port priority*).

Note: If you use the functions in this menu, then disable the flow control. The flow control is inactive if in the *Switching > Global* dialog, *Configuration* frame the *Flow control* checkbox is unmarked.

The menu contains the following dialogs:

- [QoS/Priority Global](#)
- [QoS/Priority Port Configuration](#)
- [802.1D/p Mapping](#)
- [IP DSCP Mapping](#)
- [Queue Management](#)

5.7.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

The device lets you maintain access to the device management, even in situations with heavy utilization. In this dialog, you specify the required QoS/priority settings.

Configuration

VLAN priority for management packets

Specifies the VLAN priority for sending management data packets. Depending on the VLAN priority, the device assigns the data packet to a specific *traffic class* and thus to a specific priority queue of the port.

Possible values:

0 . 7 (default setting: 0)

In the [Switching > QoS/Priority > 802.1D/p Mapping](#) dialog, you assign a *traffic class* to every VLAN priority.

IP DSCP value for management packets

Specifies the IP DSCP value for sending management data packets. Depending on the IP DSCP value, the device assigns the data packet to a specific *traffic class* and thus to a specific priority queue of the port.

Possible values:

0 (be/cs0) . . 63 (default setting: 0 (be/cs0))

Some values in the list also have a DSCP keyword, for example 0 (be/cs0), 10 (af 11) and 46 (ef). These values are compatible with the *IP Precedence* model.

In the [Switching > QoS/Priority > IP DSCP Mapping](#) dialog you assign a *traffic class* to every IP DSCP value.

Queues per port

Displays the number of priority queues per port.

The device has 8 priority queues per port. You assign every priority queue to a specific *traffic class* (*traffic class* according to IEEE 802.1D).

5.7.2 QoS/Priority Port Configuration

[Switching > QoS/Priority > Port Configuration]

In this dialog, you specify for every port how the device processes received data packets based on their QoS/priority information.

Table

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

5.7.3 802.1D/p Mapping

[Switching > QoS/Priority > 802.1D/p Mapping]

The device forwards data packets with a VLAN tag according to the contained QoS/priority information with a higher or lower priority.

In this dialog, you assign a *traffic class* to every VLAN priority. You assign the *traffic classes* to the priority queues of the ports.

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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
5	5	Video Video transmission with delays and jitter <100 ms
6	6	Voice Voice transmission with delays and jitter <10 ms
7	7	Network Control Data for network management and redundancy mechanisms

5.7.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

The device forwards IP data packets according to the DSCP value contained in the data packet with a higher or lower priority.

In this dialog, you assign a *traffic class* to every DSCP value. You assign the *traffic classes* to the priority queues of the ports.

Table

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

5.7.5 Queue Management

[Switching > QoS/Priority > Queue Management]

This dialog lets you enable and disable the *Strict priority* function for the *traffic classes*. When you disable the *Strict priority* function, the device processes the priority queues of the ports with *Weighted Fair Queuing*.

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 %.

5.8 VLAN

[Switching > VLAN]

With VLAN (Virtual Local Area Network) you distribute the data packets in the physical network to logical subnets. This provides you with the following advantages:

- High flexibility
 - With VLAN you distribute the data packets to logical networks in the existing infrastructure. Without VLAN, it would be necessary to have additional devices and complicated cabling.
 - With VLAN you specify network segments independently of the location of the individual end devices.
- Improved throughput
 - In VLANs data packets can be transferred by priority. When the priority is high, the device transfers the data of a VLAN preferentially, for example for time-sensitive applications such as VoIP phone calls.
 - When the data packets and Broadcasts are distributed in small network segments instead of in the entire network, the network load is considerably reduced.
- Increased security
 - The distribution of the data packets among individual logical networks makes unwanted accessing more difficult and strengthens the system against attacks such as MAC Flooding or MAC Spoofing.

The device supports packet-based “tagged” VLANs according to IEEE 802.1Q. The VLAN tagging in the data packet indicates the VLAN to which the data packet belongs.

The device forwards the tagged data packets of a VLAN only on ports that are assigned to the same VLAN. This reduces the network load.

The device learns the MAC addresses for every VLAN separately (independent VLAN learning).

The device prioritizes the received data stream in the following sequence:

- Voice VLAN
- Port-based VLAN

The menu contains the following dialogs:

- [VLAN Global](#)
- [VLAN Configuration](#)
- [VLAN Port](#)
- [VLAN Voice](#)

5.8.1 VLAN Global

[Switching > VLAN > Global]

This dialog lets you view general VLAN parameters for the device.

Configuration

Buttons

 Reset VLAN settings

Resets the VLAN settings of the device to the default setting.

Note that you lose your connection to the device if you have changed the VLAN for the device management in the [Basic Settings > Network > Global](#) dialog.

Max. VLAN ID

Highest ID assignable to a VLAN.

See the [Switching > VLAN > Configuration](#) dialog.

VLANs (max.)

Displays the maximum number of VLANs possible.

See the [Switching > VLAN > Configuration](#) dialog.

VLANs

Number of VLANs currently set up in the device.

See the [Switching > VLAN > Configuration](#) dialog.

The VLAN 1 is permanently set up in the device.

5.8.2 VLAN Configuration

[Switching > VLAN > Configuration]

In this dialog, you manage the VLANs. To set up a VLAN, add a further table row. There you specify for each port if it transmits data packets of the respective VLAN and if the data packets contain a VLAN tag.

You distinguish between the following VLANs:

- The user sets up static VLANs.
- The device sets up dynamic VLANs automatically and removes them if the prerequisites cease to apply.

For the following functions the device sets up dynamic VLANs:

- *MRP*: If you assign to the ring ports a non-existing VLAN, then the device sets up this VLAN.
- *MVRP*: The device sets up a VLAN based on the messages of neighboring devices.

Note: The settings are effective only if the *VLAN-unaware mode* function is inactive. See the [Switching > Global](#) dialog.

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 1..32 characters

<Port number>

Specifies if the respective port transmits data packets of the VLAN and if the data packets contain a VLAN tag.

Possible values:

- (default setting)

The port is not a member of the VLAN and does not transmit data packets of the VLAN.

T = Tagged

The port is a member of the VLAN and transmits the data packets with a VLAN tag. You use this setting for uplink ports, for example.

LT = Tagged Learned

The port is a member of the VLAN and transmits the data packets with a VLAN tag.

The device 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, the connection to the device terminates when you transfer the changes to the device. The access to the device management is possible only using the Command Line Interface through the serial interface.

5.8.3 VLAN Port

[Switching > VLAN > Port]

In this dialog, you specify how the device handles received data packets that have no VLAN tag, or whose VLAN tag differs from the VLAN ID of the port.

This dialog lets you assign a VLAN to the ports and thus specify the port VLAN ID.

Additionally, you also specify for each port how the device forwards data packets if the *VLAN-unaware mode* function is inactive and one of the following situations occurs:

- The port receives data packets without a VLAN tagging.
- The port receives data packets with VLAN priority information (VLAN ID 0, priority tagged).
- The VLAN ID in the tag of the data packet differs from the VLAN ID of the port.

Note: The settings are effective only if the *VLAN-unaware mode* function is inactive. See the *Switching > Global* dialog.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 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 *admi tAl l* 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 you specify the value 1 here for the ring ports. Otherwise, the device assigns the value to the ring ports automatically.

Acceptable packet types

Specifies if the port transmits or discards received data packets without a VLAN tag.

Possible values:

- admi tAl l* (default setting)
The port accepts data packets both with and without a VLAN tag.
- admi tOnl yVl anTagged*
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.

5.8.4 VLAN Voice

[Switching > VLAN > Voice]

Use the Voice VLAN feature to separate voice and data packets on a port, by VLAN and/or priority. A primary benefit of Voice VLAN is safeguarding the quality of voice data when the port has a high load.

The device detects VoIP phones using the Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). The device then adds the appropriate port to the member set of the set-up Voice VLAN. The member set is either tagged or untagged. Tagging depends on the Voice VLAN interface mode ([vlan](#), [dot1p-priority](#), [none](#), [untagged](#)).

Another benefit of the Voice VLAN feature is that the VoIP phone obtains VLAN ID or priority information from the device using LLDP-MED. As a result, the VoIP phone sends voice data packets with VLAN tag, priority tag or untagged. This depends on the specified Voice VLAN Interface mode. You activate Voice VLAN on the port which is connecting to the VoIP phone.

Operation

Operation

Enables/disables the [Voice](#) function of the device globally.

Possible values:

- [On](#)
- [Off](#) (default setting)

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 *multi-client* value before activating this function. You find the *Port control* parameter in the *Network Security > 802.1X > Global* dialog.

unmarked

5.9 L2-Redundancy

[Switching > L2-Redundancy]

The menu contains the following dialogs:

- MRP
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

5.9.1 MRP

[Switching > L2-Redundancy > MRP]

The Media Redundancy Protocol (MRP) is a protocol that lets you set up high-availability, ring-shaped network structures. An MRP Ring with Hirschmann devices is made up of up to 100 devices that support the Media Redundancy Protocol (MRP) according to IEC 62439.

If a section is not operating, then the ring structure of an MRP Ring changes back into a line structure. You can specify the maximum recovery time.

The *Ring Manager* device closes the ends of a backbone in a line structure to a redundant ring.

Note: *Spanning Tree* and Ring Redundancy have an effect on each other. Deactivate the *Spanning Tree* function for the ports connected to the MRP Ring. See the *Switching > L2-Redundancy > Spanning Tree > Port* dialog.

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 you 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.

VLAN ID

Specifies the VLAN ID which you assign to the ring ports.

Possible values:

0 (default setting)

No VLAN assigned.

In the *Switching > VLAN > Configuration* dialog, assign for VLAN 1 the value **U** to the ring ports.

1..4042

VLAN assigned.

If you assign a non-existing VLAN to the ring ports, then the device automatically sets up this VLAN. In the *Switching > VLAN > Configuration* dialog, the device adds a table row for the VLAN and assigns the value **T** to the ring ports.

Advanced mode

Activates/deactivates the *Advanced mode* for fast recovery times.

Possible values:

marked (default setting)

Advanced mode active.

MRP-capable Hirschmann devices support this mode.

unmarked

Advanced mode inactive.

Select this setting if another device in the ring does not support this mode.

Domain ID

Displays a sequence of 16-bytes in decimal notation, which identifies the MRP domain that the device belongs to.

Information

Information

Displays the status of the ring.

Possible values:

Redundancy available. Ring is closed.

Normal operation. The components in the ring operate as intended.

Configuration error: Error on ring port link.

The device has detected a link error on a ring port. Verify that the correct port is selected in the *Ring port 1* and *Ring port 2* frames.

Redundancy not available. Ring is open. Check the Ring clients.

The device has not detected a configuration error, but no redundancy is available.

Redundancy not available. At least one ring port is disabled.

At least one of the ring ports is disabled. Verify that both ring ports are enabled. See the *Basic Settings > Port* dialog.

Configuration error: Packets from another ring manager received.

Another device exists in the ring that operates in the *Ring Manager* mode.

Enable the *Ring manager* function only on one device in the ring.

Configuration error: Ring link is connected to wrong port.

A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on one of the ring ports.

Last time the ring was open

Displays the date and time at which the device last detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.

Number of times the ring was open

Displays the number of times the device has detected an open ring. The field displays a valid value if the device operates in the *Ring Manager* mode.

5.9.2 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.

Note: When you connect the device to the network through twisted-pair SFPs instead of through usual twisted-pair ports, the reconfiguration of the network takes slightly longer.

The menu contains the following dialogs:

- [Spanning Tree Global](#)
- [Spanning Tree Port](#)

5.9.21 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 *di sabl ed*, *di scar di ng*, *I ear ni ng*, *f or v ar di ng*.

The parameters *Forward delay [s]* and *Max age* have the following relationship:

$$\text{Forward delay [s]} = (\text{Max age}/2) + 1$$

If you enter values in the fields that contradict this relationship, then the device replaces these values with the last valid values or with the default value.

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 3x 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 *disabling*, *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 `flapping` status using the *Spanning Tree* function since the *Spanning Tree* instance was started.

Time since topology change

Displays the time since the last topology change.

Possible values:

`<days, hours: minutes: seconds>`

5.9.2.2 Spanning Tree Port

[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.

[manual Fwd](#)

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-BPDUs 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-BPDUs 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-BPDUs 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 $1.5 \times \text{Hello time [s]}$, 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 *desi gnated*.

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 $2 \times$ *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.

5.9.3 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 Link Aggregation Control Protocol (LACP) makes it possible to monitor the packet-based continuous link status on the physical ports. LACP also helps ensure that the link partners meet the aggregation prerequisites.

If the remote side does not support the Link Aggregation Control Protocol (LACP), then you can use the *Static link aggregation* function. In this case, the device aggregates the links based on the link, link speed and duplex setting.

Table

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

Buttons



Add

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

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

After you set up a LAG interface, the device adds the LAG interface to the table in the *Basic Settings > Port* dialog, *Statisticstab*.



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.

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 LACPDU and discards received LACPDU.

`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.

Track name

Displays the name of the tracking object made up of the values displayed in the *Type* and *Track ID* columns.

Active ports (min.)

Specifies the minimum number of physical ports to be active for the LAG interface to stay active. If the number of active physical ports is lower than the specified value, then the device deactivates the LAG interface.

If a redundancy function like *Spanning Tree* or *MRP* over LAG is active in the device, then you use this function to force the device to switch automatically to the redundant line.

Possible values:

1..4 (default setting: 1)

Depending on the hardware, the upper value can be greater than 4, for example 8 or 32.

Type

Displays if the LAG interface is based on the *Static link aggregation* function or on LACP.

Possible values:

`static`

The LAG interface is based on the *Static link aggregation* function.

`dynamic`

The LAG interface is based on LACP.

Send trap (Link up/down)

Activates/deactivates the sending of SNMP traps when the device detects a change in the link up/down status for this interface.

Possible values:

`marked` (default setting)

The sending of SNMP traps is active. The prerequisite is that in the [Diagnostics > Status Configuration > Alarms \(Traps\)](#) dialog the [Alarms \(Traps\)](#) function is enabled and at least one trap destination is specified.

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*.

CCL

(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

CCL

DST

DFT

EXP

For further information on the values, see the description of the *LACP actor oper state* column and IEEE 802.1AX-2014.

5.9.4 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 Backup pair configuration.

Possible values:

`marked`

The Link Backup pair is active. The device senses the link and administration status and forwards the data packets according to the pair configuration.

`unmarked` (default setting)

The Link Backup pair is inactive. The ports forward the data packets according to standard switching.

Create

Primary port

Specifies the *Primary port* of the backup interface pair. During normal operation this port is responsible for forwarding the data packets.

Possible values:

Physical ports

Backup port

Specifies the *Backup port* to which the device transfers the data packets to if the device detects an error on the *Primary port*.

Possible values:

Physical ports except for the port you set as the *Primary port*.

5.9.5 FuseNet

[Switching > L2-Redundancy > FuseNet]

The *FuseNet* protocols let you couple rings that are operating with one of the following redundancy protocols:

- MRP
- RSTP

Note: If you use the *Ring/Network Coupling* function to couple networks, then verify that the networks only contain Hirschmann devices.

Use the following table to select the *FuseNet* coupling protocol to be used in the network:

Main Ring	Connected Network	
	MRP	RSTP
MRP	<i>Sub Ring</i> ¹⁾	<i>Ring/Network Coupling</i>
RSTP	–	–

– no suitable coupling protocol

1) with the *MRP* function set up on different VLANs

The menu contains the following dialogs:

- [Sub Ring](#)
- [Ring/Network Coupling](#)

5.9.5.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub Ring]

This dialog lets you set up the device to operate in the *Sub Ring Manager* mode.

The *Sub Ring* function lets you easily couple network segments to existing redundancy rings. The *Sub Ring Manager* device couples a Sub Ring to an existing ring (base ring).

You can integrate any devices that support MRP as participants in the Sub Ring. These devices do not require support for the *Sub Ring* function.

When setting up Sub Rings, remember the following rules:

- The device supports *Link Aggregation* in the Sub Ring
- No spanning tree on Sub Ring ports
- Same *MRP domain* on devices within a Sub Ring
- Different VLANs for base ring and Sub Ring

Specify the VLAN settings as follows:

- VLAN X for base ring
 - on the ring ports of the devices participating in the base ring
 - on the base ring ports of the *Sub Ring Manager* device
- VLAN Y for Sub Ring
 - on the ring ports of the devices participating in the Sub Ring
 - on the Sub Ring ports of the *Sub Ring Manager* device

Note: To help avoid loops, only close the redundant line when the settings are specified in every device participating in the ring.

Operation

Operation

Enables/disables the *Sub Ring* function.

Possible values:

On

The *Sub Ring* function is enabled.

Off (default setting)

The *Sub Ring* function is disabled.

Information

Table entries (max.)

Displays the maximum number of Sub Rings supported by the device.

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- In the [Sub Ring ID](#) field, you specify the number that uniquely identifies the Sub Ring.

Possible values:

[1](#) . [40000](#)

You can replace the value prefilled by the device with any value in the range.

The device lets you set a maximum of 8 Sub Ring instances.



Remove

Removes the selected table row.

Sub Ring ID

Displays the number that uniquely identifies the Sub Ring.

Name

Specifies the optional name of the Sub Ring.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Active

Activates/deactivates the Sub Ring.

Activate the Sub Ring when the configuration of every device participating in the Sub Ring is complete. Close the Sub Ring only after activating the [Sub Ring](#) function.

Possible values:

[marked](#)

The Sub Ring is active.

[unmarked](#) (default setting)

The Sub Ring is inactive.

Status

Displays the operational state of the Sub Ring configuration.

Possible values:

[noError](#)

The device detects an acceptable Sub Ring configuration.

ringPortLinkError

- The ring port has no link.
- One of the Sub Ring lines is connected to one more port of the device. But the Sub Ring line is not connected to one of the ring ports of the device.

multipleSRM

The *Sub Ring Manager* device receives data packets from more than one *Sub Ring Manager* devices in the Sub Ring.

noPartnerManager

The *Sub Ring Manager* device receives its own data packets.

concurrentVLAN

The Media Redundancy Protocol (MRP) in the base ring uses the VLAN of the *Sub Ring Manager* domain.

concurrentPort

One more redundancy protocol uses the ring port of the *Sub Ring Manager* domain.

concurrentRedundancy

The *Sub Ring Manager* domain is inactive because of one more active redundancy protocol.

trunkMember

The ring port of the *Sub Ring Manager* domain is member of a *Link Aggregation* connection.

sharedVLAN

The *Sub Ring Manager* domain is inactive because shared VLAN is active and the main ring also uses the Media Redundancy Protocol (MRP).

Redundancy

Displays if the redundancy is available.

When a component of the Sub Ring becomes inoperable, the redundant line takes over its function.

Possible values:

redGuaranteed

The redundancy is available.

redNotGuaranteed

The redundancy is unavailable.

Port

Specifies the port that connects the device to the Sub Ring.

Possible values:

<Port number>

Administrative mode

Specifies the mode of the *Sub Ring Manager* device.

There are 2 *Sub-Ring Manager* devices that connect the Sub Ring to the base ring. As long as the Sub Ring is physically closed, one *Sub Ring Manager* device blocks its Sub Ring port.

Possible values:

manager (default setting)

The Sub Ring port forwards data packets.

When this value is set on both devices that couple the Sub Ring to the base ring, the device with the higher MAC address functions as the *redundant Manager*.

redundant Manager

The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets.

When this value is set on both devices that couple the Sub Ring to the base ring, the device with the higher MAC address functions as the **redundant Manager**.

single Manager

Use this value when the Sub Ring is coupled to the base ring through one single device. The prerequisite is that there are 2 instances of the Sub Ring in the table. Assign this value to both instances. The Sub Ring port of the instance with the higher port number is blocked while the Sub Ring is physically closed.

Operational mode

Displays the current mode of the *Sub Ring Manager* device.

Possible values:

manager

The Sub Ring port forwards data packets.

redundant Manager

The Sub Ring port is blocked while the Sub Ring is physically closed. If the Sub Ring is interrupted, then the Sub Ring port transmits the data packets.

single Manager

The Sub Ring is coupled to the base ring through one single device. This device blocks its Sub Ring port with the higher port number while the Sub Ring is physically closed.

disabled

The Sub Ring is inactive.

Port status

Displays the connection status on the Sub Ring port.

Possible values:

forwarding

The port is passing frames according to the forwarding behavior of IEEE 802.1D.

disabled

The port is dropping every frame.

blocked

The port is dropping every frame with the exception of the following cases:

- The port passes frames used by the selected ring protocol specified to pass blocked ports.
- The port passes frames from other protocols specified to pass blocked ports.

not-connected

The port link is interrupted.

Sub Ring status

Displays the operational state of the Sub Ring in the *Sub Ring Manager* domain.

Possible values:

undefined

Undefined state

open

The Sub Ring is opened.

closed

The Sub Ring is closed.

VLAN

Specifies the VLAN to which this Sub Ring is assigned. If no VLAN exists with the specified VLAN ID, then the device sets up the VLAN.

Possible values:

Available set-up VLANs (default setting: 0)

If you do not want to use a separate VLAN for this Sub Ring, then you keep the value as 0.

Partner MAC

Displays the MAC address of the *Sub Ring Manager* device at the other end of the Sub Ring.

MRP domain

Specifies the MRP domain of the *Sub Ring Manager* device. Assign the same MRP domain name to every member of a Sub Ring. If you only use Hirschmann devices, then you use the default value for the MRP domain; otherwise adjust this value if necessary. With multiple Sub Rings, the function lets you use the same MRP domain name for the Sub Rings.

Possible values:

Permitted MRP domain names (default setting:

255. 255. 255. 255. 255. 255. 255. 255. 255. 255. 255. 255. 255. 255)

Protocol

Specifies the protocol.

Possible values:

i ec-62439-mrp

5.9.5.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > Ring/Network Coupling]

You use the [Ring/Network Coupling](#) function to redundantly couple an existing HIPER Ring, MRP Ring, or Fast HIPER Ring to another network or another ring. Verify that the coupling partners are Hirschmann devices.

Note: With two-switch coupling, verify that you have set up a HIPER Ring, MRP Ring, or Fast HIPER Ring before setting up the [Ring/Network Coupling](#) function.

In the [Switching > L2-Redundancy > FuseNet > Ring/Network Coupling](#) dialog, you can perform the following tasks:

- display an overview of the existing [Ring/Network Coupling](#)
- set up a [Ring/Network Coupling](#) instance
- enable/disable the [Ring/Network Coupling](#) instance
- delete the [Ring/Network Coupling](#) instance

When configuring the coupling ports, specify the following settings in the [Basic Settings > Port](#) dialog:

| Port type | Bit rate | Port on | Autoneg | Manual configuration |
|-----------|------------|---------|----------|----------------------|
| TX | 100 Mbit/s | marked | unmarked | 100MFDX |
| TX | 1 Gbit/s | marked | marked | – |
| Optical | 100 Mbit/s | marked | unmarked | 100MFDX |
| Optical | 1 Gbit/s | marked | marked | – |

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

If you set up VLANs, then note the VLAN configuration of the coupling and partner coupling ports. Specify the following settings for the coupling and partner coupling ports:

- [Switching > VLAN > Port](#) dialog
 - Value in the [Port-VLAN ID](#) column = 1
 - Checkbox in the [Ingress filtering](#) column = unmarked
- [Switching > VLAN > Configuration](#) dialog
 - VLAN membership = T

Independently of the VLAN settings, the device sends the ring coupling frames with VLAN ID 1 and priority 7. Verify that the device sends VLAN 1 frames tagged in the local ring and in the connected network. Tagging the VLAN frames maintains the priority of the ring coupling frames.

The [Ring/Network Coupling](#) function operates with test packets. The devices send their test packets with a VLAN tag, including VLAN ID 1 and the highest VLAN priority 7. If the unblocked port is a member in VLAN 1 and transmits the data packets without a VLAN tag, then the device also sends test packets.

Operation

Buttons



Reset

Disables the redundancy function and resets the parameters in the dialog to the default setting.

Operation

Enables/disables the *Ring/Network Coupling* function.

Possible values:

On

The *Ring/Network Coupling* function is enabled.

Off (default setting)

The *Ring/Network Coupling* function is disabled.

Information

Redundancy

Displays if the redundancy is available.

When a component of the ring becomes inoperable, the redundant line takes over its function.

Possible values:

redGuaranteed

The redundancy is available.

redNotGuaranteed

The redundancy is unavailable.

Configuration failure

You have set up the function incorrectly, or there is no ring port connection.

Possible values:

noError

slaveCouplingLinkError

The coupling line is not connected to the coupling port of the slave device. Instead, the coupling line is connected to another port of the slave device.

slaveControlLinkError

The control port of the slave device has no data link.

masterControlLinkError

The control line is not connected to the control port of the master device. Instead, the control line is connected to another port of the master device.

twoSlaves

The control line connects two slave devices.

localPartnerLinkError

The partner coupling line is not connected to the partner coupling port of the slave device. Instead, the partner coupling line is connected to another port of the slave device in *one-switch coupling* mode.

localInvalidCouplingPort

In *one-switch coupling* mode, the coupling line is not connected on the same device as the partner line. Instead, the coupling line is connected to another device.

couplingPortNotAvailable

The coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.

controlPortNotAvailable

The control port is not available because the module to which the port refers is not available or the port does not exist on this module.

partnerPortNotAvailable

The partner coupling port is not available because the module to which the port refers is not available or the port does not exist on this module.

Mode

Type

Specifies the method used to couple the networks together.

Possible values:

one-switch coupling (default setting)

Lets you specify the port settings in the *Coupling port* and *Partner coupling port* frames.

two-switch coupling, master

Lets you specify the port settings in the *Coupling port* frame.

two-switch coupling with control line, master

Lets you specify the port settings in the *Coupling port* and *Control port* frames.

two-switch coupling, slave

Lets you specify the port settings in the *Coupling port* frame.

two-switch coupling with control line, slave

Lets you specify the port settings in the *Coupling port* and *Control port* frames.

Coupling port

Port

Specifies the port to which you connect the redundant link.

Possible values:

-

No port selected.

<Port number>

If you also have set up ring ports, then specify the coupling and ring ports on different ports.

To help prevent continuous loops, the device disables the coupling port in the following cases:

- disabling the function
- changing the configuration while the connections are operating on the ports

When the device has deactivated the coupling port, the *Port on* checkbox is unmarked in the *Basic Settings > Port* dialog, *Configuration* tab.

State

Displays the status of the selected port.

Possible values:

[active](#)

The port is active.

[standby](#)

The port is in stand-by mode.

[not-connected](#)

The port is not connected.

[not-appl i cabl e](#)

The port is incompatible with the set-up control mode.

Partner coupling port

Port

Specifies the port on which you connect the partner port. The field is visible when you select the [one-sw i tch coupl i ng](#) radio button in the *Mode* frame.

Possible values:

- (default setting)

No port selected.

<Port number >

If you also have set up ring ports, then specify the coupling and ring ports on different ports.

Interface index

Displays the index number of the port that the partner device uses for the connection. The field is visible when you select a two-switch coupling method in the *Mode* frame.

State

Displays the status of the selected port.

Possible values:

[active](#)

The port is active.

[standby](#)

The port is in stand-by mode.

[not-connected](#)

The port is not connected.

[not-appl i cabl e](#)

The port is incompatible with the set-up control mode.

IP address

Displays the IP address of the partner device, when the devices are connected. The prerequisite is that you enable the partner device in the network. The field is visible when you select a two-switch coupling method in the *Mode* frame.

Control port

Port

Displays the port on which you connect the control line.

Possible values:

- (default setting)
No port selected.
- <Port number>

State

Displays the status of the selected port.

Possible values:

- [active](#)
The port is active.
- [standby](#)
The port is in stand-by mode.
- [not-connected](#)
The port is not connected.
- [not-applicable](#)
The port is incompatible with the set-up control mode.

Configuration

Redundancy mode

Specifies if the device responds to a detected failure in the remote ring or network.

Possible values:

- [redundant ring/network coupling](#)
Either the main line or the redundant line is active. Both lines are not active simultaneously. If the device detects that the link is interrupted between the devices in the remote ring or network, then the standby device keeps the redundant port in the standby mode.
- [extended redundancy](#) (default setting)
If the device detects a potential connection interruption between the devices in the remote ring or network, then the standby device forwards data on the redundant port. In this case, the main line and the redundant line are active simultaneously. This setting lets you maintain continuity in the remote network.

Note: During the reconfiguration period, package duplications can occur. Therefore, if your application is able to detect package duplications, then you can select this setting.

Coupling mode

Specifies the mode of coupling a specific type of network.

Possible values:

[ring coupling](#) (default setting)

The device couples redundant rings. The device lets you couple rings that use the following redundancy protocols:

- MRP Ring

[network coupling](#)

The device couples network segments. The function lets you couple mesh and bus networks together.

6 Diagnostics

The menu contains the following dialogs:

- [Status Configuration](#)
- [System](#)
- [Email Notification](#)
- [Syslog](#)
- [Ports](#)
- [LLDP](#)
- [Loop Protection](#)
- [Report](#)

6.1 Status Configuration

[Diagnostics > Status Configuration]

The menu contains the following dialogs:

- [Device Status](#)
- [Security Status](#)
- [Signal Contact](#)
- [MAC Notification](#)
- [Alarms \(Traps\)](#)

6.1.1 Device Status

[Diagnostics > Status Configuration > Device Status]

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device to present its condition in graphic form.

The device displays its current status as `error` or `ok` in the *Device status* frame. The device determines this status from the individual monitoring results.

The device displays detected faults in the *Status* tab and also in the *Basic Settings > System* dialog, *Device status* frame.

The dialog contains the following tabs:

- [Global]
- [Port]
- [Status]

[Global]

Device status

Device status

Displays the current status of the device. The device determines the status from the individual monitored parameters.

Possible values:

`ok`

`error`

The device displays this value to indicate a detected error in one of the monitored parameters.

Traps

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function.

Possible values:

`marked` (default setting)

The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.

If the device detects a change in the monitored functions, then the device sends an SNMP trap.

`unmarked`

The sending of SNMP traps is inactive.

Table

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

Ethernet module removal

Activates/deactivates the monitoring of the Ethernet modules.

Possible values:

marked

Monitoring is active.

If you remove an Ethernet module from the device, then in the *Device status* frame, the value changes to *error*.

Further below, you have the option of selecting the Ethernet modules to be monitored individually.

unmarked (default setting)

Monitoring is inactive.

External memory removal

Activates/deactivates the monitoring of the active external memory.

Possible values:

`marked`

Monitoring is active.

If you remove the active external memory from the device, then in the *Device status* frame, the value changes to `error`.

`unmarked` (default setting)

Monitoring is inactive.

External memory not in sync

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

`marked`

Monitoring is active.

In the *Device status* frame, the value changes to `error` in the following situations:

- The configuration profile only exists in the device.
- The configuration profile in the device differs from the configuration profile in the external memory.

`unmarked` (default setting)

Monitoring is inactive.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

`marked`

Monitoring is active.

In the *Device status* frame, the value changes to `error` in the following situations:

- The redundancy function becomes active (loss of redundancy reserve).
- The device is a normal ring participant and detects an error in its settings.

`unmarked` (default setting)

Monitoring is inactive.

Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:

`marked` (default setting)

Monitoring is active.

If the device has a detected power supply fault, then in the *Device status* frame, the value changes to `error`.

`unmarked`

Monitoring is inactive.

Ethernet module

Activates/deactivates the monitoring of this Ethernet module.

Possible values:

`marked`

Monitoring is active.

If you remove the module from the device, then in the *Device status* frame, the value changes to `error`.

`unmarked` (default setting)

Monitoring is inactive.

This setting is effective when you mark the *Ethernet module removal* checkbox further up.

[Port]**Table**

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

Port

Displays the port number.

Propagate connection error

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

Possible values:

`marked`

Monitoring is active.

If the link on the selected port/interface is interrupted, then in the *Device status* frame, the value changes to `error`.

`unmarked` (default setting)

Monitoring is inactive.

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

[Status]**Table**

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

Timestamp

Displays the date and time of the event in the format, `Month Day, Year hh:mm:ss AMPM`

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 with serial interface possible

Activates/deactivates the monitoring of the system monitor.

When the system monitor is active, you have the possibility to change to the system monitor using a serial connection during the system startup.

Possible values:

`marked`

Monitoring is active.

If you activate the system monitor, then in the *Security status* frame, the value changes to `error`.

`unmarked` (default setting)

Monitoring is inactive.

You activate/deactivate the system monitor in the *Diagnostics > System > Selftest* dialog.

Saving the configuration profile on the external memory possible

Activates/deactivates the monitoring of the configuration profile in the external memory.

Possible values:

`marked`

Monitoring is active.

If you activate the saving of the configuration profile in the external memory, then in the *Security status* frame, the value changes to `error`.

`unmarked` (default setting)

Monitoring is inactive.

You activate/deactivate the saving of the configuration profile in the external memory in the *Basic Settings > External Memory* dialog.

Link interrupted on enabled device ports

Activates/deactivates the monitoring of the link on the active ports.

Possible values:

`marked`

Monitoring is active.

If the link interrupts on an active port, then in the *Security status* frame, the value changes to `error`. In the *Port* tab, you have the option of selecting the ports to be monitored individually.

`unmarked` (default setting)

Monitoring is inactive.

Access with HiDiscovery possible

Activates/deactivates the monitoring of the HiDiscovery function.

Possible values:

`marked` (default setting)

Monitoring is active.

If you enable the HiDiscovery function, then in the *Security status* frame, the value changes to `error`.

`unmarked`

Monitoring is inactive.

You enable/disable the HiDiscovery function in the *Basic Settings > Network > Global* dialog.

Load unencrypted config from external memory

Activates/deactivates the monitoring of loading unencrypted configuration profiles from the external memory.

Possible values:

`marked` (default setting)

Monitoring is active.

If the settings allow the device to load an unencrypted configuration profile from the external memory, then in the *Security status* frame, the value changes to `error`.

If the following preconditions are fulfilled, then the *Security status* frame in the *Basic Settings > System* dialog, displays an alarm.

- The configuration profile stored in the external memory is unencrypted.
and

- The *Config priority* column in the *Basic Settings > External Memory* dialog has the value `first`.

`unmarked`

Monitoring is inactive.

IEC61850-MMS active

Activates/deactivates the monitoring of the *IEC61850-MMS* function.

Possible values:

marked (default setting)

Monitoring is active.

If you enable the *IEC61850-MMS* function, then in the *Security status* frame, the value changes to *error*.

unmarked

Monitoring is inactive.

You enable/disable the *IEC61850-MMS* function in the *Advanced > Industrial Protocols > IEC61850-MMS* dialog, *Operation* frame.

Self-signed HTTPS certificate present

Activates/deactivates the monitoring of the 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.

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 in the format, `Month Day, Year hh:mm:ss AMPM`

Cause

Displays the event which caused the SNMP trap.

6.1.3 Signal Contact

[Diagnostics > Status Configuration > Signal Contact]

The signal contact is a potential-free relay contact. The device thus lets you perform remote diagnosis. The device uses the relay contact to signal the occurrence of events by opening the relay contact and interrupting the closed circuit.

Note: The device can contain several signal contacts. Each contact contains the same monitoring functions. Several contacts allow you to group various functions together providing flexibility in system monitoring.

The menu contains the following dialogs:

- [Signal Contact 1 / Signal Contact 2](#)

6.1.3.1 Signal Contact 1 /Signal Contact 2

[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1]

In this dialog, you specify the trigger conditions for the signal contact.

The signal contact gives you the following options:

- Monitoring the correct operation of the device.
- Signaling the device status of the device.
- Signaling the security status of the device.
- Controlling external devices by manually setting the signal contacts.

The device displays detected faults in the [Status](#) tab and also in the [Basic Settings > System](#) dialog, [Signal contact status](#) frame.

The dialog contains the following tabs:

- [\[Global\]](#)
- [\[Port\]](#)
- [\[Status\]](#)

[Global]

Configuration

Mode

Specifies which events the signal contact indicates.

Possible values:

[Manual setting](#) (default setting for [Signal Contact 2](#), if present)

You use this setting to manually open or close the signal contact, for example to turn on or off a remote device. See the [Contact](#) option list.

[Monitoring correct operation](#) (default setting)

Using this setting the signal contact indicates the status of the parameters specified in the table below.

[Device status](#)

Using this setting the signal contact indicates the status of the parameters monitored in the [Diagnostics > Status Configuration > Device Status](#) dialog. In addition, you can read the status in the [Signal contact status](#) frame.

[Security status](#)

Using this setting the signal contact indicates the status of the parameters monitored in the [Diagnostics > Status Configuration > Security Status](#) dialog. In addition, you can read the status in the [Signal contact status](#) frame.

[Device/Security status](#)

Using this setting the signal contact indicates the status of the parameters monitored in the [Diagnostics > Status Configuration > Device Status](#) and the [Diagnostics > Status Configuration > Security Status](#) dialog. In addition, you can read the status in the [Signal contact status](#) frame.

Contact

Toggles the signal contact manually. The prerequisite is that from the *Mode* drop-down list the *Manual setting* item is selected.

Possible values:

open

The signal contact is opened.

close

The signal contact is closed.

Signal contact status

Signal contact status

Displays the current status of the signal contact.

Possible values:

Opened (error)

The signal contact is opened. The circuit is interrupted.

Closed (ok)

The signal contact is closed. The circuit is closed.

Trap configuration

Send trap

Activates/deactivates the sending of SNMP traps when the device detects a change in a monitored function.

Possible values:

marked

The sending of SNMP traps is active. The prerequisite is that in the *Diagnostics > Status Configuration > Alarms (Traps)* dialog the *Alarms (Traps)* function is enabled and at least one trap destination is specified.

If the device detects a change in the monitored functions, then the device sends an SNMP trap.

unmarked (default setting)

The sending of SNMP traps is inactive.

Table

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

Connection errors

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

Possible values:

[marked](#)

Monitoring is active.

If the link interrupts on a monitored port/interface, then the signal contact opens.

In the [Port](#) tab, you have the option of selecting the ports/interfaces to be monitored individually.

[unmarked](#) (default setting)

Monitoring is inactive.

Temperature

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

Possible values:

[marked](#) (default setting)

Monitoring is active.

If the temperature exceeds the specified upper threshold value or falls below the specified lower threshold value, then the signal contact opens.

[unmarked](#)

Monitoring is inactive.

You specify the temperature threshold values in the [Basic Settings > System](#) dialog, [Upper temp. limit \[°C\]](#) field and [Lower temp. limit \[°C\]](#) field.

Ethernet module removal

Activates/deactivates the monitoring of the Ethernet modules.

Possible values:

[marked](#)

Monitoring is active.

If you remove an Ethernet module from the device, then the signal contact opens.

Further below, you have the option of selecting the Ethernet modules to be monitored individually.

[unmarked](#) (default setting)

Monitoring is inactive.

External memory removed

Activates/deactivates the monitoring of the active external memory.

Possible values:

[marked](#)

Monitoring is active.

If you remove the active external memory from the device, then the signal contact opens.

[unmarked](#) (default setting)

Monitoring is inactive.

External memory not in sync with NVM

Activates/deactivates the monitoring of the configuration profile in the device and in the external memory.

Possible values:

`marked`

Monitoring is active.

The signal contact opens in the following situations:

- The configuration profile only exists in the device.
- The configuration profile in the device differs from the configuration profile in the external memory.

`unmarked` (default setting)

Monitoring is inactive.

Ring redundancy

Activates/deactivates the monitoring of the ring redundancy.

Possible values:

`marked`

Monitoring is active.

The signal contact opens in the following situations:

- The redundancy function becomes active (loss of redundancy reserve).
- The device is a normal ring participant and detects an error in its settings.

`unmarked` (default setting)

Monitoring is inactive.

Ethernet loops

Activates/deactivates the monitoring of layer 2 Ethernet loops. You specify the settings for the [Loop Protection](#) function in the [Diagnostics > Loop Protection](#) dialog.

Possible values:

`marked`

Monitoring is active.

If the device has detected an Ethernet loop, then the signal contact opens.

`unmarked` (default setting)

Monitoring is inactive.

Power supply

Activates/deactivates the monitoring of the power supply unit.

Possible values:

`marked` (default setting)

Monitoring is active.

If the device has a detected power supply fault, then the signal contact opens.

`unmarked`

Monitoring is inactive.

Ethernet module

Activates/deactivates the monitoring of this Ethernet module.

Possible values:

[marked](#)

Monitoring is active.

If you remove this Ethernet module from the device, then the signal contact opens.

[unmarked](#) (default setting)

Monitoring is inactive.

This setting is effective when you mark the [Ethernet module removal](#) checkbox further up.

[Port]**Table**

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

Port

Displays the port number.

Propagate connection error

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

Possible values:

[marked](#)

Monitoring is active.

If the link interrupts on the selected port/interface, then the signal contact opens.

[unmarked](#) (default setting)

Monitoring is inactive.

This setting takes effect when you mark the [Connection errors](#) checkbox in the [Global](#) tab.

[Status]**Table**

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

Timestamp

Displays the date and time of the event in the format, [Month Day, Year](#) [hh:mm:ss AM/PM](#)

Cause

Displays the event which caused the SNMP trap.

6.1.4 MAC Notification

[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 ($2^{31} - 1$) (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.

6.1.5 Alarms (Traps)

[[Diagnostics](#) > [Status Configuration](#) > [Alarms \(Traps\)](#)]

The device lets you send an SNMP trap in response to specific events.

You specify the events for which the device triggers an SNMP trap in the following dialogs:

- [Diagnostics](#) > [Status Configuration](#) > [Device Status](#)
- [Diagnostics](#) > [Status Configuration](#) > [Security Status](#)
- [Diagnostics](#) > [Status Configuration](#) > [MAC Notification](#)

The menu contains the following dialogs:

- [Trap V3 User Management](#)
- [Trap Destinations](#)

6.1.5.1 Trap V3 User Management

[Diagnostics > Status Configuration > Alarms (Traps) > Trap V3 User Management]

In this dialog, you specify the SNMPv3 trap users who can send SNMP traps to the trap destination(s). The device supports encrypted SNMPv3 traps and authentication for sending.

SNMPv3 trap users have permission to send SNMPv3 traps to the specified SNMPv3 trap hosts.

SNMPv3 trap users are intended for sending SNMPv3 traps to SNMPv3 trap hosts exclusively. SNMPv3 trap users are different from the user accounts set up in the device. Do not confuse them. See the [Device Security > User Management](#) dialog.

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row. The device adds an SNMPv3 trap user 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 protocol for sending SNMPv3 traps with authentication.
Possible values:
[none](#)
The device sends SNMPv3 traps unencrypted and without authentication.
[hmacmd5](#)
The device sends SNMPv3 traps using the Message-Digest Algorithm 5 (HMACMD5) protocol.
Available if this protocol is already set for the user to be cloned.
[hmacsha](#)
The device sends SNMPv3 traps using the Secure Hash Algorithm (HMACSHA) protocol.
Available if this protocol is already set for the user to be cloned.
- In the [Trap User Auth Password](#) field, you specify the password that the SNMPv3 trap user uses to authenticate before sending.
Possible values:
Alphanumeric ASCII character string with 8..64 characters
The prerequisite is that from the [Trap User Auth Protocol](#) drop-down list, an item other than [none](#) is selected.
- From the [Trap User Priv Protocol](#) drop-down list, you select the protocol that the device uses for this user to encrypt the SNMPv3 traps.
Possible values:
[none](#) (default setting)
No encryption.

*des**Data Encryption Standard (DES).*

Available if this protocol is already set for the user to be cloned.

*aesCfb128**Advanced Encryption Standard (AES128).*

Available if this protocol is already set for the user to be cloned.

- In the *Trap User Priv Password* field, you specify the password that the SNMPv3 trap user uses to authenticate before sending.

Possible values:

Alphanumeric ASCII character string with 8..64 characters

The prerequisite is that from the *Trap User Auth Protocol* drop-down list, an item other than *none* is selected.

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

Displays ***** (asterisks) instead of the authentication password of the SNMPv3 trap user.

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

Displays ***** (asterisks) instead of the password that the SNMPv3 trap user uses to authenticate before sending.

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.

6.1.5.2 Trap Destinations

[Diagnostics > Status Configuration > Alarms (Traps) > Trap Destinations]

In this dialog, you specify the trap destinations to which the device sends SNMP traps.

For SNMPv3, the following conditions apply:

- The device sends SNMPv3 traps to the trap destination specified for the relevant SNMPv3 trap user.
- The device supports a maximum of 10 trap destinations for SNMPv3.

Operation

Operation

Enables/disables sending SNMP traps.

Possible values:

- On** (default setting)
Sending SNMP traps is enabled.
- Off**
Sending SNMP traps is disabled.

SNMPv1/v2 trap community

Name

Specifies the community string that the device sends in each SNMPv1/v2 trap for authentication to the trap destination.

Possible values:

- Alphanumeric ASCII character string with 0..64 characters
- trap** (default setting)

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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
For security reasons, we recommend not to use this setting.
 - V3*
SNMP version 3
- In the *Address* field, you specify the IP address and the port of the trap destination.
Possible values:
 - <I Pv4 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:
 - noAuthNoPri v*
The device sends SNMPv3 traps unencrypted without authentication.
For security reasons, we recommend not to use this setting.
 - authNoPri v*
The device sends SNMPv3 traps unencrypted.
The user needs to authenticate before sending SNMPv3 traps.
 - authPri v*
The device sends SNMPv3 traps encrypted.
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:

<I Pv4 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 SNMPv3 traps unencrypted without authentication.
For security reasons, we recommend not to use this setting.

[authNoPriv](#)

The device sends SNMPv3 traps unencrypted.
The user needs to authenticate before sending SNMPv3 traps.

[authPriv](#)

The device sends SNMPv3 traps encrypted.
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](#)

6.21 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.

6.22 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.

6.24 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.

6.25 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

Removes the dynamically set up addresses from the ARP table.

Port

Displays the port number.

IP address

Displays the IPv4 address or the IPv6 address of a neighboring device.

MAC address

Displays the MAC address of a neighboring device.

Last updated

Displays the time in seconds since the current settings of the entry were registered in the ARP table.

Type

Displays the type of the entry.

Possible values:

`static`

Static entry. When the ARP table is deleted, the device keeps the static entry.

`dynamic`

Dynamic entry. When the *Aging time [s]* has been exceeded and the device does not receive any data from this device during this time, the device deletes the dynamic entry.

`local`

IP and MAC address of the device management.

Active

Displays that the ARP table contains the IP/MAC address assignment as an active entry.

6.26 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 changing to the system monitor during the system startup.
- Specify how the device behaves in the case of a detected error.

Configuration

If the device does not detect any readable configuration profile when restarting, then the following settings block your access to the device permanently.

- *SysMon1 is available* checkbox is **unmarked**.
- *Load default config on error* checkbox is **unmarked**.

This is the case, for example, if the password of the configuration profile that you are loading differs from the password set in the device. To have the device unlocked again, contact your sales partner.

RAM test

Activates/deactivates the RAM memory check 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 changing to the system monitor during the system startup.

Possible values:

marked (default setting)

The device lets you change to the system monitor during the system startup.

unmarked

The device starts without the option of changing to the system monitor.

Among other things, the system monitor lets you update the device software and to delete saved configuration profiles.

Load default config on error

Activates/deactivates the loading of the default settings if the device does not detect any readable configuration profile when restarting.

Possible values:

`marked` (default setting)

The device loads the default settings.

`unmarked`

The device interrupts the restart and stops. The access to the device management is possible only using the Command Line Interface through the serial interface.

To regain the access to the device through the network, open the system monitor and reset the settings. 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 Email Notification

[Diagnostics > Email Notification]

The device lets you inform multiple recipients by email about events that have occurred.

The device sends the emails immediately or periodically depending on the event severity. Usually you specify events with a high severity to be sent immediately.

You can specify multiple recipients to which the device sends the emails either immediately or periodically.

The menu contains the following dialogs:

- [Email Notification Global](#)
- [Email Notification Recipients](#)
- [Email Notification Mail Server](#)

6.3.1 Email Notification Global

[Diagnostics > Email Notification > Global]

In this dialog, you specify the sender settings. Also, you specify for which event severities the device sends the emails immediately and for which periodically.

Operation

Operation

Enables/disables the sending of emails:

Possible values:

On

The sending of emails is enabled.

Off (default setting)

The sending of emails is disabled.

Information

Buttons



Clear email notification statistics

Resets the counters in the *Information* frame to 0.

Sent messages

Displays how many times the device has successfully sent an email to the mail server.

Undeliverable messages

Displays how many times the device has unsuccessfully tried to send an email to the mail server.

Time of the last messages sent

Displays the date and time at which the device has last sent an email to the mail server.

Certificates/CRLs

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

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

Buttons

 Clear all Certificates/CRLs

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

URL

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


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

- X.509 format
- . PEMfile name extension
- Base64-coded and enclosed by the lines


```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
or
-----BEGIN CRL-----
...
-----END CRL-----
```

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

- Import from the PC

When the file is located on your PC or on a network drive, drag and drop it onto the  area. As an alternative, click in the area to select the file.
- Import from an FTP server

This option is not recommended 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 from a TFTP server
This option is not recommended 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 from an SCP or SFTP server
When the file is on an SCP or SFTP server, specify the URL for the file in the following form:
`scp://` or `sftp://<IP address>/<path>/<file name>`
Click the [Start](#) button to open the [Credentials](#) window. In this window, you enter the [User name](#) and [Password](#) to log into the server.
`scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`
Remember to set up the SCP or SFTP server as an SSH known host before the device accesses the server for the first time. See the [Device Security > SSH Known Hosts](#) dialog.

Start

Transfers the file specified in the [URL](#) field onto the device.

In this dialog, you can transfer a maximum of 20 digital certificates and additionally a maximum of 20 CRLs onto the device.

For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the [Email Notification](#) function. See the [Operation](#) frame.

Sender

Email address

Specifies the email address of the device.

The device sends the emails using this email address as the sender.

Possible values:

Alphanumeric ASCII character string with 0..255 characters
(default setting: `switch@chirschmann.com`)

Notification urgent

Here you specify the settings for emails which the device sends immediately.

Severity

Specifies the minimum severity of events for which the device immediately sends an email. If an event of this severity occurs, or of a more urgent severity, then the device sends an email to the recipients.

Possible values:

[emergency](#)
[alert](#) (default setting)
[critical](#)
[error](#)
[warning](#)

noti ce
i nformati onal
debug

Subject

Specifies the subject of the email.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Notification non-urgent

Here you specify the settings for emails which the device sends periodically.

Severity

Specifies the minimum severity of events for which the device periodically sends an email. If an event of this severity occurs, or of a more urgent severity, then the device registers the event in the buffer. The device sends the buffer content periodically or when the buffer overflows.

If an event of a less urgent severity occurs, then the device does not register the event in the buffer.

Possible values:

emer gency
al er t
cri ti cal
error
var ni ng (default setting)
noti ce
i nformati onal
debug

Subject

Specifies the subject of the email.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Sending interval [min]

Specifies the send interval in minutes.

If the device has registered at least one event, then the device sends an email with the log file after the time expires.

Possible values:

30 . 1440 (default setting: 30)

Send

Sends an email immediately with the buffer content and clears the buffer.

Meaning of the event severities

| Severity | Meaning |
|---------------|--------------------------------------|
| emergency | Device not ready for operation |
| alert | Immediate user intervention required |
| critical | Critical status |
| error | Error status |
| warning | Warning |
| notice | Significant, normal status |
| informational | Information message |
| debug | Debug message |

6.3.2 Email Notification Recipients

[Diagnostics > Email Notification > Recipients]

In this dialog, you specify the recipients to which the device sends the emails. The device lets you specify up to 10 recipients.

Table

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

Buttons



Add

Adds a table row.



Remove

Removes the selected table row.

Index

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

Notification type

Specifies whether the device sends the emails to this recipient immediately or periodically.

Possible values:

[urgent](#) (default setting)

The device sends the emails to this recipient immediately.

[non-urgent](#)

The device sends the emails to this recipient periodically.

Email address

Specifies the email address of the recipient.

Possible values:

Valid email address with up to 255 characters

Active

Activates/deactivates the informing of the recipient.

Possible values:

[marked](#)

The informing of the recipient is active.

[unmarked](#) (default setting)

The informing of the recipient is inactive.

6.3.3 Email Notification Mail Server

[Diagnosics > Email Notification > Mail Server]

In this dialog, you specify the settings for the mail servers. The device supports encrypted and unencrypted connections to the mail server.

Table

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

Buttons



Add

Adds a table row.



Remove

Removes the selected table row.



Connection test

Opens the [Connection test](#) window to send a test email.

If the mail server settings are correct, then the selected recipients receive a test email.

- From the [Recipient](#) drop-down list, you select to which recipients the device sends the test email.
Possible values:
 - [urgent](#)
The device sends the test email to the recipients to which the device sends emails immediately.
 - [non-urgent](#)
The device sends the test email to the recipients to which the device sends emails periodically.
- In the [Message text](#) field, you specify the text of the test email.

Index

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

Description

Specifies the name of the server.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

IP address

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

Possible values:

Valid IPv4 address (default setting: 0.0.0.0)

Valid IPv6 address

DNS name in the format <domain>. <tl d> or <host>. <domain>. <tl d>

The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.

To establish an encrypted connection using a digital certificate, verify that the *Common Name* or *Subject Alternative Name* information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

Destination TCP port

Specifies the TCP port of the server.

Possible values:

1..65535 (2¹⁶ - 1) (default setting: 25)

Exception: Port 2222 is reserved for internal functions.

Frequently used TCP-Ports:

- SMTP 25
- Message Submission 587

Encryption

Specifies the protocol which encrypts the connection between the device and the mail server.

Possible values:

none (default setting)

The device establishes an unencrypted connection to the server.

tlsv1

The device establishes an encrypted connection to the server using the startTLS extension.

User name

Specifies the user name of the account which the device uses to authenticate on the mail server.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Password

Specifies the password of the account which the device uses to authenticate on the mail server.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Timeout [s]

Specifies the time in seconds after which the device sends an email again. The prerequisite is that the device was unsuccessful at sending the complete email due to a connection error.

Possible values:

1..15 (default setting: 3)

Active

Activates/deactivates the use of the mail server.

Possible values:

marked

The mail server is active.

The device sends emails to this mail server.

unmarked (default setting)

The mail server is inactive.

The device does not send emails to this mail server.

6.4 Syslog

[Diagnostics > Syslog]

The device lets you report selected events, independent of the severity of the event, to different syslog servers.

In this dialog, you specify the settings for this function and manage up to 8 syslog servers.

Operation

Operation

Enables/disables the sending of events to the syslog servers.

Possible values:

On

The sending of events is enabled.

The device sends the events specified in the table to the specified syslog servers.

Off (default setting)

The sending of events is disabled.

Certificates/CRLs

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

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

Buttons

 Clear all Certificates/CRLs

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

URL

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

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

- X.509 format
- . PEM/file name extension
- Base64-coded and enclosed by the lines

```
-----BEGIN CERTIFICATE-----
```

```
...
```

```
-----END CERTIFICATE-----
```


or

```
-----BEGIN CRL-----
```

```
...
```

```
-----END CRL-----
```

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

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

Start

Transfers the file specified in the [URL](#) field onto the device.

In this dialog, you can transfer a maximum of 32 digital certificates and additionally a maximum of 32 CRLs onto the device.

For the changes to take effect after transferring a digital certificate or a CRL into the device, disable and re-enable the [Syslog](#) function. See the [Operation](#) frame.

Table

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

DNS name in the format <domain>. <tl d> or <host>. <domain>. <tl d>

The prerequisite is that you also enable the *Client* function in the *Advanced > DNS > Client > Global* dialog.

To establish an encrypted connection using a digital certificate, verify that the *Common Name* or *Subject Alternative Name* information in the digital certificate that you have transferred onto the device matches the value you specify here. Otherwise, the device will not be able to verify the identity of the server.

Destination UDP port

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

Possible values:

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

Transport type

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

Possible values:

udp (default setting)

The device sends the events over the UDP port specified in the *Destination UDP port* column.

tls

The device sends the events over TLS on the TCP port specified in the *Destination UDP port* column.

Min. severity

Specifies the minimum severity of the events. The device sends a log entry for events with this severity and with more urgent severities to the syslog server.

Possible values:

emergency

alert

critical

error

warning (default setting)

notice
informational
debug

Type

Specifies the type of the log entry transmitted by the device.

Possible values:

systemlog (default setting)
audittrail

Active

Activates/deactivates the transmission of events to the syslog server.

Possible values:

marked
The device sends events to the syslog server.
unmarked (default setting)
The transmission of events to the syslog server is deactivated.

6.5 Ports

[Diagnostics > Ports]

The menu contains the following dialogs:

- [SFP](#)
- [TP cable diagnosis](#)
- [Port Monitor](#)
- [Auto-Disable](#)
- [Port Mirroring](#)

6.5.1 SFP

[Diagnostics > Ports > SFP]

This dialog lets you look at the SFP transceivers currently connected to the device and their properties.

Table

The table displays valid values if the device is equipped with SFP transceivers.

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

Port

Displays the port number.

Module type

Type of the SFP transceiver, for example M-SFP-SX/LC.

Serial number

Displays the serial number of the SFP transceiver.

Connector type

Displays the connector type.

Supported

Displays if the device supports the SFP transceiver.

Temperature [°C]

Operating temperature of the SFP transceiver in °Celsius.

Tx power [mW]

Transmission power of the SFP transceiver in mW.

Rx power [mW]

Receiving power of the SFP transceiver in mW.

Tx power [dBm]

Transmission power of the SFP transceiver in dBm.

Rx power [dBm]

Receiving power of the SFP transceiver in dBm.

6.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

This feature tests the cable attached to an interface for short or open circuit. The table displays the cable status and estimated length. The device also displays the individual cable pairs connected to the port. When the device detects a short circuit or a broken cable, it also displays the estimated distance to where it detected the problem.

To receive dependable results, use the *TP cable diagnosis* function for twisted-pair cables with a minimum length of 10 meters.

Note: This test temporarily interrupts the data stream on the port.

Information

Port

Displays the port number.

Start cable diagnosis...

Opens the *Select port* window.

From the *Port* drop-down list you select the port to be tested. Use for copper-based ports only.

To initiate the cable test on the selected port, click the *Ok* button.

Status

Status of the Virtual Cable Tester.

Possible values:

active

Cable testing is in progress.

To start the test, click the *Start cable diagnosis...* button. This action opens the *Select port* window.

success

The device successfully performed a test.

failure

The device detected that the test was interrupted.

uninitialized

The device has not performed any test yet.

Table

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

6.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

The *Port Monitor* function monitors the adherence to the specified parameters on the ports. If the *Port Monitor* function detects that the parameters are being exceeded, then the device performs an action.

To apply the *Port Monitor* function, perform the following steps:

- *Global* tab
 - Enable the *Port Monitor* function in the *Operation* frame.
 - Activate for each port those parameters that you want the *Port Monitor* function to monitor.
- *Link flap*, *CRC/Fragments* and *Overload detection* tabs
 - Specify the threshold values for the parameters for each port.
- *Link speed/Duplex mode detection* tab
 - Activate the allowed combinations of speed and duplex mode for each port.
- *Global* tab
 - Specify for each port an action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.
- *Auto-disable* tab
 - Mark the *Auto-disable* checkbox for the monitored parameters if you have specified the *auto-disable* action at least once.

The dialog contains the following tabs:

- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

[Global]

In this tab you enable the *Port Monitor* function and specify the parameters that the *Port Monitor* function is monitoring. Also specify the action that the device carries out if the *Port Monitor* function detects that the parameters have been exceeded.

Operation

Operation

Enables/disables the *Port Monitor* function globally.

Possible values:

On

The *Port Monitor* function is enabled.

Off (default setting)

The *Port Monitor* function is disabled.

Table

For information on how to customize the appearance of the table, see [“Working with tables” on page 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 3x 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 3x 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.

[not Present](#)

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 (10) (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 \(10 \)](#) (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 \(10 \)](#) (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.

6.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

The *Auto-Disable* function lets you disable monitored ports automatically and enable them again as you desire.

For example, the *Port Monitor* function and selected functions in the *Network Security* menu use the *Auto-Disable* function to disable ports if monitored parameters are exceeded.

If the parameters are no longer being exceeded, then the *Auto-Disable* function enables the relevant port again after the specified waiting period.

The dialog contains the following tabs:

- [Port]
- [Status]

[Port]

This tab displays which ports are currently disabled due to the parameters being exceeded. If the parameters are no longer being exceeded and you specify a waiting period in the *Reset timer [s]* column, then the *Auto-Disable* function automatically enables the relevant port again.

Table

For information on how to customize the appearance of the table, see “Working with tables” on page 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 ($2^{32} - 1$)

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.

Loop protection

A layer 2 network loop detected on the port. See the [Diagnostics > Loop Protection](#) dialog, [Loop detected](#) column.

Active

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

Possible values:

marked

The port is currently disabled.

unmarked

The port is enabled.

[Status]

This tab displays the monitored parameters for which the [Auto-Disable](#) function is active.

Table

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

Reason

Displays the parameters that the device monitors.

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

Category

Displays which function the adjacent parameter belongs to.

Possible values:

port monitor

The parameter belongs to the functions in the [Diagnostics > Ports > Port Monitor](#) dialog.

network security

The parameter belongs to the functions in the [Network Security](#) dialog.

L2 redundancy

The parameter belongs to the functions in the [Switching > L2-Redundancy](#) dialog or to the [Loop Protection](#) function, see the [Diagnostics > Loop Protection](#) dialog.

Auto-disable

Displays if the *Auto-Disable* function is active/inactive for the adjacent parameter.

Possible values:

marked

The *Auto-Disable* function for the adjacent parameters is active.

The *Auto-Disable* function disables and, when applicable, enables the relevant port again if the monitored parameters are exceeded.

unmarked (default setting)

The *Auto-Disable* function for the adjacent parameters is inactive.

6.5.5 Port Mirroring

[Diagnostics > Ports > Port Mirroring]

The *Port Mirroring* function lets you copy received and sent data packets from selected ports to a destination port. You can watch and process the data stream using an analyzer or an *RMON probe*, connected to the destination port. The data packets remain unmodified on the source port.

Note: To enable the access to the device management using the destination port, mark the checkbox *Allow management* in the *Destination port* frame before you enable the *Port Mirroring* function.

Operation

Buttons



Reset config

Resets the settings in the dialog to the default settings and restores the previously applied settings.

Operation

Enables/disables the *Port Mirroring* function.

Possible values:

On

The *Port Mirroring* function is enabled.

The device copies the data packets from the selected source ports to the destination port.

Off (default setting)

The *Port Mirroring* function is disabled.

Destination port

Primary port

Specifies the destination port.

Suitable ports are those ports that are not used for the following purposes:

- Source port
- Uplink port on which a Layer 2 redundancy protocol is active

Possible values:

- (default setting)

No destination port selected.

<Port number>

Number of the destination port. The device copies the data packets from the source ports to this port.

On the destination port, the device adds a VLAN tag to the data packets that the source port sends. The destination port sends the unmodified data packets that the source port receives.

Note: The destination port needs sufficient bandwidth to absorb the data stream. If the copied data stream exceeds the bandwidth of the destination port, then the device discards superfluous data packets on the destination port.

Secondary port

Specifies a second destination port. The prerequisite is that you have specified a primary port.

Possible values:

- (default setting)

No destination port selected.

<Port number >

Number of the destination port. The device copies the data packets from the source ports to this port.

Allow management

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

Possible values:

marked

The access to the device management using the destination port is active.

The device lets users have access to the device management using the destination port without interrupting the active *Port Mirroring* session.

- The device duplicates multicasts, broadcasts and unknown unicasts on the destination port.
- The VLAN settings on the destination port remain unchanged. The prerequisite for access to the device management using the destination port is that the destination port is not a member of the VLAN of the device management.

unmarked (default setting)

The access to the device management using the destination port is inactive.

The device prohibits the access to the device management using the destination port.

Table

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

Source port

Displays the port number.

Enabled

Activates/deactivates the copying of the data packets from this source port to the destination port.

Possible values:

marked

The copying of the data packets is active.

The port is specified as a source port.

`unmarked` (default setting)

The copying of the data packets is inactive.

(Grayed-out display)

It is not possible to copy the data packets for this port.

Possible causes:

- The port is already specified as a destination port.
- The port is a logical port, not a physical port.

Note: The device lets you activate every physical port as source port except for the destination port.

Type

Specifies which data packets the device copies to the destination port.

On the destination port, the device adds a VLAN tag to the data packets that the source port sends. The destination port sends the unmodified data packets that the source port receives.

Possible values:

`none` (default setting)

No data packets.

`tx`

Data packets that the source port sends.

`rx`

Data packets that the source port receives.

`txrx`

Data packets that the source port sends.

Note: With the `txrx` setting the device copies each transmitted data packet. The destination ports needs at least a bandwidth that corresponds to the sum of the send and receive channel of the source ports. For example, for similar ports the destination port is at 100 % capacity when the send and receive channel of a source port are at 50 % capacity respectively.

6.6 LLDP

[Diagnostics > LLDP]

The device lets you gather information about neighboring devices. For this, the device uses the Link Layer Discovery Protocol (LLDP). This information lets a network management station map the structure of the network.

This menu lets you set up the topology discovery and to display the information received in tabular form.

The menu contains the following dialogs:

- [LLDP Configuration](#)
- [LLDP Topology Discovery](#)

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

This dialog lets you set up the topology discovery for every port.

Operation

Operation

Enables/disables the *LLDP* function.

Possible values:

On (default setting)

The *LLDP* function is enabled.

The topology discovery using LLDP is active in the device.

Off

The *LLDP* function is disabled.

Configuration

Transmit interval [s]

Specifies the interval in seconds at which the device sends LLDP data packets.

Possible values:

5 . 32768 (2¹⁶) (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.

6.6.2 LLDP Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

Devices in networks send notifications in the form of packets which are also known as "LLDPDU" (LLDP data units). The data that is sent and received through LLDPDUs is useful for many reasons. Thus the device detects which devices in the network are neighbors and through which ports they are connected.

The dialog lets you display the network and to detect the connected devices along with their specific features.

The dialog contains the following tabs:

- [LLDP]
- [LLDP-MED]

[LLDP]

This tab displays the collected LLDP information for the neighboring devices. This information lets a network management station map the structure of the network.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

When only devices without active topology discovery are connected to a port, the table contains one line for this port to represent every device. This line contains the number of connected devices.

The MAC address table (forwarding database) contains MAC addresses of devices that the topology table hides for the sake of clarity.

When you use one port to connect several devices, for example through a hub, the table shows one line for each connected device.

Table

For information on how to customize the appearance of the table, see ["Working with tables" on page 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:

[not Defined](#)

The device has capabilities not covered by any of the [LLDP-MED](#) classes.

[endpointClass1](#)

The device has [endpointClass1](#) capabilities.

[endpointClass2](#)

The device has [endpointClass2](#) capabilities.

[endpointClass3](#)

The device has [endpointClass3](#) capabilities.

[networkConnectivity](#)

The device has network connectivity device capabilities.

VLAN ID

Displays the extension of the VLAN Identifier for the remote system connected to this port, as defined in IEEE 802.3.

- [0](#)

Priority tagged packets

Only the 802.1D priority is significant and the device uses the default VLAN ID of the ingress port.

- [1..4042](#)

Valid Port VLAN ID

Priority

Displays the value of the *802.1D Priority* which is associated with the remote system connected to the port.

DSCP

Displays the value of the *Differentiated Service Code Point (DSCP)* which is associated with the remote system connected to the port.

Unknown bit status

Displays the *Unknown Bit Status* of incoming data packets.

Possible values:

`true`

The network policy for the specified application type is currently unknown. In this case, the device ignores the Layer 2 priority and value of the *DSCP* field.

`false`

Indicates a specified network policy.

Tagged bit status

Displays the tagged bit status.

Possible values:

`true`

The application uses a tagged VLAN.

`false`

For the specific application the device uses untagged VLAN operation. In this case, the device ignores both the VLAN ID and the Layer 2 priority fields. The DSCP value on Layer 3, however, is relevant.

Hardware revision

Displays the vendor-specific hardware revision string as advertised by the remote endpoint.

Firmware revision

Displays the vendor-specific firmware revision string as advertised by the remote endpoint.

Software revision

Displays the vendor-specific software revision string as advertised by the remote endpoint.

Serial number

Displays the vendor-specific serial number as advertised by the remote endpoint.

Manufacturer name

Displays the vendor-specific manufacturer name as advertised by the remote endpoint.

Model name

Displays the vendor-specific model name as advertised by the remote endpoint.

Asset ID

Displays the vendor-specific asset tracking identifier as advertised by the remote endpoint.

6.7 Loop Protection

[Diagnostics > Loop Protection]

The [Loop Protection](#) function helps protect against layer 2 network loops.

A network loop can lead to a standstill of the network due to overload. A possible reason is the continuous duplication of data packets due to a misconfiguration. The cause could be, for example, a poorly connected cable or an incorrect setting in the device.

For example, a layer 2 network loop can occur in the following cases, if no redundancy protocols are active:

- Two ports of the same device are directly connected to each other.
- More than one active connection is established between two devices.

In redundant network topologies, multiple redundancy protocols are typically active. You usually disable the [Spanning Tree](#) function on the ports involved in other redundancy protocols. The redundancy protocols already help to avoid loops.

Operation

Operation

Enables/disables the [Loop Protection](#) function.

Possible values:

On

The [Loop Protection](#) function is enabled.

- On active and passive ports, the device evaluates received *loop detection* packets. On active ports, the device sends *loop detection* packets at regular intervals as specified in the [Transmit interval](#) field. The prerequisite is that the [Loop Protection](#) function is active on the port.
- The device lets you monitor Ethernet loops with the signal contact. See the [Diagnostics > Status Configuration > Signal Contact > Signal Contact 1](#) dialog, checkbox for the [Ethernet loops](#) parameter.

Off (default setting)

The [Loop Protection](#) function is disabled.

The device neither sends *loop detection* packets nor evaluates received *loop detection* packets.

Configuration

Auto-disable

Activates/deactivates the *Auto-Disable* function for *Loop Protection*.

Possible values:

marked

The *Auto-Disable* function for *Loop Protection* is active.

The prerequisite for disabling the port is that in the *Action* column the value *auto-disable* or *all* is specified.

The device lets you specify the waiting period in seconds after which the *Auto-Disable* function enables the port again. To do this, in the *Diagnostics > Ports > Auto-Disable* dialog, specify the waiting period in the *Reset timer [s]* column.

unmarked (default setting)

The *Auto-Disable* function for *Loop Protection* is inactive.

Global

Transmit interval

Specifies the interval in seconds at which the device sends *loop detection* packets if the *Loop Protection* function is active on the port.

Possible values:

1..10 (default setting: 5)

Receive threshold

Specifies the threshold value for the number of consecutive *loop detection* packets received. If the number reaches or exceeds this threshold value, then the device will perform the action specified in the *Action* column.

Possible values:

1..50 (default setting: 1)

Table

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

Buttons



Clear port statistics

Resets the values in the following columns:

- *Loops*
- *Sent frames*
- *Received frames*

Port

Displays the port number.

Active

Activates/deactivates the *Loop Protection* function on the port.

Possible values:

marked

The *Loop Protection* function is active on the port.

Activate the function only on ports which are not part of a redundant network path. This helps avoid an accidental shutdown of redundant network paths.

If the device receives a *loop detection* packet on this port, sent from another port on the same device, then the device performs the action specified in the *Action* column.

unmarked (default setting)

The *Loop Protection* function is inactive on the port. The port neither sends *loop detection* packets nor evaluates received *loop detection* packets.

Mode

Specifies the behavior of the *Loop Protection* function on the port.

Possible values:

active

The device sends *loop detection* packets and evaluates received *loop detection* packets.

passive (default setting)

The device evaluates received *loop detection* packets.

Action

Specifies the action the device performs when it detects a layer 2 network loop on this port.

Possible values:

trap

The device sends a trap.

auto-disable (default setting)

The device disables the port using the *Auto-Disable* function.

The prerequisite for disabling the port is that in the *Configuration* frame the *Auto-disable* checkbox is marked.

all

The device sends a trap. Then the device disables the port using the *Auto-Disable* function.

The prerequisite for disabling the port is that in the *Configuration* frame the *Auto-disable* checkbox is marked.

VLAN ID

Specifies the VLAN in which the device sends the *loop detection* packets.

Possible values:

0 (default setting)

The device sends the *loop detection* packets without a VLAN tag.

1..4042

The device sends the *loop detection* packets in the specified VLAN. The prerequisite is that in the *Switching > VLAN > Port* dialog the VLAN is already set up and that the port is a member of the VLAN.

Loop detected

Displays if the device has detected a layer 2 network loop on the port.

Possible values:

[yes](#)

The device has detected a layer 2 network loop on the port.

After the loop has ended and the port is enabled again, the device resets the value to [no](#).

[no](#)

The device has not detected a layer 2 network loop on the port.

Loops

Displays the number of loops the device has detected on the port since the last port statistics reset or since the last system startup.

Last loop time

Displays the time at which the device detected the last loop on the port.

The prerequisite for the correct evaluation of the value is that in the [Time > Basic Settings](#) dialog the system time of the device is synchronized with the appropriate reference time.

Sent frames

Displays the number of *loop detection* packets sent on the port since the last port statistics reset or since the last system startup.

Received frames

Displays the number of sent and received back *loop detection* packets on the port since the last port statistics reset or since the last system startup.

Discarded frames

Displays the number of discarded *loop detection* packets on the port.

Examples of reasons for discarded packets:

- The device detects packets with an incorrect format.
- The device detects packets with expired timestamps (packets received more than 5 seconds after sending).
- The device received a data packet with an unexpected VLAN information.
- The device detects received packets on a port that is disabled.

6.8 Report

[Diagnostics > Report]

The menu contains the following dialogs:

- [Report Global](#)
- [Persistent Logging](#)
- [System Log](#)
- [Audit Trail](#)

6.8.1 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 363](#).

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 363](#).

The device outputs the messages on the serial interface.

Possible values:

emergency

al er t

cri ti cal

error

var ni ng (default setting)

noti ce

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 363](#).

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 363](#).

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 363](#).

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 <i>Audit Trail</i> 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 <code>show running-config script</code> . |
| 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 |

6.8.2 Persistent Logging

[Diagnostics > Report > Persistent Logging]

The device lets you save log entries permanently in a file in the external memory. Therefore, even after the device is restarted you have access to the log entries.

In this dialog, you limit the size of the log file and specify the minimum severity for the events to be saved. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly generated file.

In the table the device displays you the log files held in the external memory. As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files. This helps ensure that there is enough memory space in the external memory.

Note: Verify that an external memory is connected. To verify if an external memory is connected, see the *Status* column in the *Basic Settings > External Memory* dialog. We recommend to monitor the external memory connection using the *Device Status* function, see the *External memory removal* parameter in the *Diagnostics > Status Configuration > Device Status* dialog.

Operation

Operation

Enables/disables the *Persistent Logging* function.

Only activate this function if the external memory is available in the device.

Possible values:

On (default setting)

The *Persistent Logging* function is enabled.

The device saves the log entries in a file in the external memory.

Off

The *Persistent Logging* function is disabled.

Configuration

Max. file size [kbyte]

Specifies the maximum size of the log file in KBytes. When the log file reaches the specified size, the device archives this file and saves the following log entries in a newly 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.

As soon as the specified maximum number of files has been attained, the device deletes the oldest file and renames the remaining files.

Possible values:

0 . 25 (default setting: 4)

The value 0 deactivates saving of log entries in the log file.

Severity

Specifies the minimum severity of the events. The device saves the log entry for events with this severity and with more urgent severities in the log file in the external memory.

Possible values:

emergency
alert
critical
error
warning (default setting)
notice
informational
debug

Log file target

Specifies the external memory device for logging.

Possible values:

usb
External USB memory (ACA21/ACA22)

Table

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

Buttons

 Clear persistent log file

Removes the log files from the external memory.

Index

Displays the index number to which the table row relates.

Possible values:

1..25

The device automatically assigns this number.

File name

Displays the file name of the log file in the external memory.

Possible values:

messages

messages.X

File size [byte]

Displays the size of the log file in the external memory in bytes.

6.8.3 System Log

[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.

6.8.4 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 `showcommands`
- 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
- Opening and closing of SNMP through an HTTPS tunnel

The device does not log passwords. The logged entries are write-protected and remain saved in the device after a restart.

Note: During the system startup, access to the system monitor is possible using the default settings of the device. If an attacker gains physical access to the device, then he is able to reset the device settings to its default values using the system monitor. After this, the device and log file are accessible using the standard password. Take appropriate measures to restrict physical access to the device. Otherwise, deactivate access to the system monitor. See the [Diagnostics > System > Selftest](#) dialog, [SysMon1 is available](#) checkbox.

Buttons



Save audit trail file

Saves the HTML page on your PC using the web browser dialog.

7 Advanced

The menu contains the following dialogs:

- [DHCP](#)
- [DNS](#)
- [Industrial Protocols](#)
- [Tracking](#)
- [Command Line Interface](#)

7.1 DHCP

[Advanced > DHCP]

The menu contains the following dialogs:

- [DHCP Server](#)
- [DHCP L2 Relay](#)

7.1.1 DHCP Server

[Advanced > DHCP > DHCP Server]

The Dynamic Host Configuration Protocol (DHCP) lets a server assign the IP settings to the devices on the network (clients). The DHCP server stores and assigns the available IP addresses and further settings, if specified.

The DHCP server in the device listens for requests on UDP port 67 and responds to the client devices on UDP port 68. When the device receives a DHCP request, it validates the IP address to be assigned before leasing the IP address and other IP settings to the requesting client device.

The menu contains the following dialogs:

- [DHCP Server Global](#)
- [DHCP Server Pool](#)
- [DHCP Server Lease Table](#)

7.1.1.1 DHCP Server Global

[Advanced > DHCP > DHCP Server > Global]

This dialog lets you activate the *DHCP Server* function either globally or per port according to your requirements.

Operation

Operation

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

Possible values:

On

Off (default setting)

Configuration

IP probe

Activates/deactivates the probing for unique IP addresses. Before assigning an IP address, the device sends an *ICMP echo request* packet to check whether this IP address is already in use on the network.

Possible values:

marked (default setting)

The *IP probe* function is active.

unmarked

The *IP probe* function is inactive.

Table

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

Port

Displays the number of the physical port on which the device listens for DHCP requests and responds 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:

- *Client ID*
- *Remote ID*
- *Circuit 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 a smart way to automatically set up client devices as they obtain their IP settings. The device lets you specify such parameters for each pool.

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 DHCP request.

Possible values:

- (default setting)

The device ignores the parameter during assignment of an IP address from the pool.

Sequence of hexadecimal character pairs with 1..254 pairs separated by a space.

Example: 41 42 43 44 4F

Circuit ID

Specifies the *circuit ID*. The DHCP relay inserts the *circuit ID* into the DHCP request.

Possible values:

- (default setting)

The device ignores the parameter during assignment of an IP address from the pool.

Sequence of hexadecimal character pairs with 1..254 pairs separated by a space.

Example: 41 42 43 44 4F

Hirschmann device

Activates/deactivates the Hirschmann multicasts. If the device in this IP address range serves only 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 protocol to be used as well as the name and path of the configuration file.

Possible values:

Alphanumeric ASCII character string with 0..70 characters

Example: `ftp://192.9.200.1/config.xml`

When you leave this field blank, the device leaves this option field blank in the DHCP message.

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)

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.

[offer ing](#)

The DHCP server is validating that the IP address is suitable for the client.

[requesti ng](#)

The DHCP client is acquiring the offered IP address.

[bound](#)

The DHCP server is leasing the IP address to a client.

[renewi ng](#)

The DHCP client is requesting an extension to the lease.

[rebi ndi ng](#)

The DHCP server is assigning the IP address to the client after a successful renewal.

[decl i ned](#)

The DHCP server denied the request for the IP address.

[rel eased](#)

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](#)

7.21 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 DNS

[Advanced > DNS]

The menu contains the following dialogs:

- [DNS Client](#)

7.3.1 DNS Client

[Advanced > DNS > Client]

DNS (Domain Name System) is a service in the network that translates hostnames into IP addresses. This name resolution lets you contact other devices using their hostnames instead of their IP addresses.

Using the *Client* function the device sends requests for resolving hostnames in IP addresses to a DNS server.

The menu contains the following dialogs:

- [DNS Client Global](#)
- [DNS Client Current](#)
- [DNS Client Static](#)
- [DNS Client Static Hosts](#)

7.3.1.1 DNS Client Global

[Advanced > DNS > Client > Global]

In this dialog, you enable the *Client* function and the *Cache* function.

Operation

Operation

Enables/disables the *Client* function.

Possible values:

On

The *Client* function is enabled.

The device sends requests for resolving hostnames in IP addresses to a DNS server.

Off (default setting)

The *Client* function is disabled.

Cache

Buttons



Flush cache

Deletes every entry from the DNS cache.

Cache

Enables/disables the *Cache* function.

Possible values:

On (default setting)

The *Cache* function is enabled.

The device caches up to 128 DNS server responses (hostname and corresponding IP address).

When the cache contains a matching entry, the hostname of a new request the device resolves itself. This makes sending a new query to the DNS server unnecessary.

Off

The *Cache* function is disabled.

7.3.1.2 DNS Client Current

[Advanced > DNS > Client > Current]

This dialog displays to which DNS servers the device sends requests for resolving hostnames in IP addresses.

Table

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

Index

Displays the sequential number of the DNS server.

Address

Displays the IP address of the DNS server. The device forwards requests for resolving hostnames in IP addresses to the DNS server with this IP address.

7.3.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

In this dialog, you specify the DNS servers to which the device forwards requests for resolving hostnames in IP addresses.

The device lets you specify up to 4 IP addresses yourself or to transfer the IP addresses from a DHCP server.

Configuration

Source

Specifies the source from which the device obtains the IP address of DNS servers to which the device addresses requests.

Possible values:

[user](#)

The device uses the IP addresses specified in the table.

[nrgnt - dhcp](#) (default setting)

The device uses the IP addresses which the DHCP server delivers to the device.

Domain name

Specifies the domain name according to RFC 1034 which the device adds to hostnames without a domain suffix.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Request timeout [s]

Specifies the time interval in seconds for sending again a request to the server.

Possible values:

[0](#)

Deactivates the function. The device does not send a request to the server again.

[1..3600](#) (default setting: [3](#))

Request retransmits

Specifies, how many times the device retransmits a request.

The prerequisite is that in the [Request timeout \[s\]](#) field a value [>0](#) is specified.

Possible values:

0 . 100 (default setting: 2)

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- In the [Index](#) field, you specify the index number.
Possible values:
 - 1 . 4
The device lets you specify up to 4 external DNS servers.
- In the [IP address](#) field, you specify the IP address of the DNS server.
Possible values:
 - Valid IPv4 address
 - Valid IPv6 address



Remove

Removes the selected table row.

Index

Displays the sequential number of the DNS server. You specify the index number when you add a table row.

IP address

Specifies the IP address of the DNS server.

Possible values:

Valid IPv4 address

Valid IPv6 address

Active

Activates/deactivates the table row.

Prerequisites:

- In the [Advanced > DNS > Client > Global](#) dialog the *DNS client* function is enabled.
- In the [Configuration](#) frame, the item [user](#) is selected from the [Source](#) drop-down list.

Possible values:

marked (default setting)

The table row is active.

The device sends requests to the DNS server specified in the first active table row. When the device does not receive a response from this server, it sends the requests to the DNS server specified in the next active table row. The relevant timeout is specified in the [Configuration](#) frame, [Request timeout \[s\]](#) field.

unmarked

The table row is inactive.

The device does not send requests to this DNS server.

7.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

This dialog lets you specify up to 64 hostnames which you link with one IP address each. Upon a request for resolving hostnames in IP addresses, the device searches this table for a corresponding entry. When the device does not find a corresponding entry, it forwards the request.

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- In the [Index](#) field, you specify the index number.
Possible values:
 - 1..64
The device lets you specify up to 64 static hosts.
- In the [Name](#) field, you specify the hostname of the related device.
Possible values:
 - Alphanumeric ASCII character string with 1..255 characters
- In the [IP address](#) field, you specify the IP address of the related device.
Possible values:
 - Valid IPv4 address
 - Valid IPv6 address



Remove

Removes the selected table row.

Index

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

Name

Specifies the hostname.

Possible values:

Alphanumeric ASCII character string with 1..255 characters

IP address

Specifies the IP address under which the host is reachable.

Possible values:

Valid IPv4 address

Valid IPv6 address

Active

Activates/deactivates the table row.

Possible values:

marked (default setting)

The table row is active.

When the device receives a request for this hostname, it provides the requesting client device with the associated IP address.

unmarked

The table row is inactive.

When the device receives a DNS request for this hostname, it forwards the request to a DNS server specified in the [Advanced > DNS > Client > Static](#) dialog.

7.4 Industrial Protocols

[Advanced > Industrial Protocols]

The menu contains the following dialogs:

- [IEC61850-MMS](#)
- [Modbus TCP](#)
- [OPC UA Server](#)
- [Service Discovery](#)

7.4.1 IEC61850-MMS

[Advanced > Industrial Protocols > IEC61850-MMS]

The IEC61850-MMS is a standardized industrial communication protocol from the International Electrotechnical Commission (IEC). For example, automatic switching equipment uses this protocol when communicating with power station equipment.

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

Note: IEC61850/MMS does not provide any authentication mechanisms. If the write access for IEC61850/MMS is activated, then every client that can access the device using TCP/IP is capable of changing the settings of the device. 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 *IEC61850-MMS* server.

Possible values:

On

The *IEC61850-MMS* server is enabled.

Off (default setting)

The *IEC61850-MMS* server is disabled.

The IEC61850 MIBs stay accessible.

Information

Status

Displays the current *IEC61850-MMS* server status.

Possible values:

unavailable

starting

running

stopping

halted
error

Active sessions

Displays the number of active MMS server connections.

Configuration

Buttons

 Download ICD file

Copies the ICD file to your PC.

Write access

Activates/deactivates the write access to the MMS server.

Possible values:

[marked](#)

The write access to the MMS server is activated. This setting lets you change the device settings using the IEC 61850 MMS protocol.

[unmarked](#) (default setting)

The write access to the MMS server is deactivated. The MMS server is accessible as read-only.

Technical key

Specifies the IED name.


The IED name is eligible independently of the system name.

Possible values:

Alphanumeric ASCII character string with 0..32 characters

The device accepts the following characters:

- [0](#) . [9](#)
- [a](#) . [z](#)
- [A](#) . [Z](#) (default setting: [KEY](#))

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

TCP port

Specifies TCP port for MMS server access.

Possible values:

[1](#) . [65535](#) ($2^1 - 1$) (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)

7.4.2 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 an unavoidable security risk, because the protocol does not authenticate user access.

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

Operation

Operation

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

Possible values:

On

The *Modbus TCP* server is enabled.

Off (default setting)

The *Modbus TCP* server is disabled.

Configuration

Write access

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

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

Possible values:

`marked` (default setting)

The *Modbus TCP* server read/write access is active. This lets you change the device 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`)

7.4.3 OPC UA Server

[Advanced > Industrial Protocols > OPC UA Server]

The protocol *OPC UA* is a standardized protocol for industrial communication defined in the standard IEC 62541. The *OPC UA Server* function monitors the *OPC UA* information model data for the industrial automation equipments such as Programmable Logic Controllers (PLC), sensors and meters.

To monitor the *OPC UA* information model data of the connected end devices, use an *OPC UA* client application.

In this dialog, you enable the *OPC UA Server* function and specify the required settings. You can also specify the number of sessions allowed to be open at the same time. The dialog lets you manage the *OPC UA* user accounts required to access the device using a *OPC UA* client application. Every *OPC UA* user requires an active *OPC UA* user account to gain access to the *OPC UA* server of the device.

Operation

Operation

Enables/disables the *OPC UA Server* function in the device.

Possible values:

On

The *OPC UA Server* function is enabled.

Off (default setting)

The *OPC UA Server* function is disabled.

Configuration

Listening port

Specifies the TCP port number that the *OPC UA Server* server uses for communication.

Possible values:

1.. 65535 (2¹⁶ - 1) (default setting: 4840)

Exception: Port 2222 is reserved for internal functions.

Sessions (max.)

Specifies the maximum number of *OPC UA* connections to the device that can be set up simultaneously. Each accessing *OPC UA* client application establishes a separate *OPC UA* connection to the device.

Possible values:

1..5 (default setting: 5)

Security policy

Specifies the authentication and encryption protocol that the device applies for the *OPC UA* user.

Possible values:

`none` (default setting)

The *OPC UA* user does not need to authenticate oneself.

`basi c128Rsa15`

The *OPC UA* user authenticates using the *Basic128Rsa15* protocol.

`basi c256`

The *OPC UA* user authenticates using the *Basic256* protocol.

`basi c256Sha256`

The *OPC UA* user authenticates using the *Basic256Sha256* protocol.

Table

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

Buttons



Add

Opens the *Create* window to add a table row. The device lets you specify up to 4 *OPC UA* user accounts.

- In the *User name* field, you specify the name of the *OPC UA* user account.

Possible values:

Alphanumeric ASCII character string with 1..32 characters

The device accepts the following characters:

a..z

A..Z

0..9

<space>

-_



Remove

Removes the selected table row.

User name

Displays the name of the *OPC UA* user having access to the device using an *OPC UA* client application.

Password

Specifies the password that the user applies to access the device using an *OPC UA* client application.

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

Possible values:

Alphanumeric ASCII character string with 6..64 characters

The device accepts the following characters:

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

Access role

Specifies the role that regulates the access of the *OPC UA* user using an *OPC UA* client application.

Possible values:

`readOnly` (default setting)

The *OPC UA* user account has read-only access to the device. The *OPC UA* user can view the *OPC UA* information model data of the connected end devices.

Active

Activates/deactivates the *OPC UA* user account in the device.

Possible values:

`marked`

The *OPC UA* user account is active. The device accepts the login of an *OPC UA* user with this user name.

`unmarked` (default setting)

The *OPC UA* user account is inactive. The device rejects the login of an *OPC UA* user with this user name.

7.4.4 Service Discovery

[Advanced > Industrial Protocols > Service Discovery]

Service Discovery is part of a series of technologies summarized by the term Zero-configuration networking (zeroconf). Service Discovery uses multicast DNS (mDNS) and DNS service discovery (DNS-SD) to advertise the services offered by the device to other devices in the network that request the service. The device currently supports the *ITxPT Module Inventory* service. Additional services may follow in future releases.

Devices that support Service Discovery can automatically discover the available services on the network without having information about which devices are available. In public transportation, for example, such devices can be ticketing systems, passenger information systems, or vehicle tracking systems.

Devices that subscribe to the services will detect a new device as soon as you connect it to the network, and read its service data. For example, when you install a ticketing system in the network of a public transportation vehicle, the ticketing system needs to communicate with the existing passenger information system to deliver real-time updates on ticket sales and availability.

In this dialog, you select and set up the services that the device will advertise.

The dialog contains the following tabs:

- [\[ITxPT Module Inventory\]](#)

[ITxPT Module Inventory]

The *ITxPT Module Inventory* service is part of the Information Technology for Public Transport (ITxPT) specification.

The intended use of the *ITxPT Module Inventory* service is module inventory in networks of vehicles. The *ITxPT Module Inventory* service lets devices subscribing to the service automatically inventory the modules installed in the on-board IP network of vehicles. Modules in the sense of ITxPT might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system. The service lets you collect information about the modules and monitor their status.

The device provides the information through *SRV records* and *TXT records*.

- The *SRV record* contains the location.
- The device provides the *TXT record* through mDNS.
The *TXT record* contains information about the service.

The device transmits the *TXT record* once in the following cases:

- After an mDNS query containing the address `_i t x p t _ s o c k e t . _ t c p . l o c a l .`
The device transmits the *TXT record* in response to multicast or unicast requests in the network for services offered by the device.
- Without a request
 - As soon as the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled. See the *Operation* frame.
 - If the *Service Discovery* function and the *ITxPT Module Inventory* service are enabled, and the device detects changes regarding the global status or the port status of other devices in the network. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

Operation

Operation

Enables/disables the *Service Discovery* function. Simultaneously, the device activates/deactivates the *ITxPT Module Inventory* service to monitor the link status or the PoE status of the device.

Possible values:

On

The *Service Discovery* function is enabled.

The *ITxPT Module Inventory* service is active.

The device performs the following actions:

- On ports for which the checkbox in the *Link* column is marked:
Monitoring the link status.
Writing the link status into the *xstatus* attribute of the *TXT record*.
- On ports for which the checkbox in the *PoE* column is marked:
Monitoring the PoE status.
Writing the PoE status into the *xstatus* attribute of the *TXT record*.
- The device sends the *TXT record* one time to the devices subscribing to this service.

The device sends the *TXT record* without a request in the following cases:

- When you enable the *Service Discovery* function.
or
- When the device detects a change regarding the global status or the port status of other devices in the network. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

Off (default setting)

The *Service Discovery* function and the *ITxPT Module Inventory* service are disabled.

Table

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

Port

Displays the port number.

Link

Activates/deactivates the *ITxPT Module Inventory* service to monitor the link status of this port.

Possible values:

marked

The device performs the following actions:

- Monitoring the link status of this port.
- Writing the link status into the *xstatus* attribute of the *TXT record*.
- Transmitting the *TXT record* once, without a request being required.

Other devices subscribing to this service data can analyze the data contained in the *TXT record*. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

unmarked (default setting)

The device does not monitor the link status of this port.

PoE

Activates/deactivates the *ITxPT Module Inventory* service to monitor the PoE status of this port.

Possible values:

marked

The device performs the following actions:

- Monitoring the PoE status of this port.
- Writing the PoE status into the *xstatus* attribute of the *TXT record*.
- Transmitting the *TXT record* once, without a request being required.

Other devices subscribing to this service data can analyze the data contained in the *TXT record*. Other devices might be other Hirschmann devices or devices from the on-board network of the vehicle. For example, the on-board passenger information system.

unmarked (default setting)

The device does not monitor the PoE status of this port.

7.5 Tracking


[Advanced > Tracking]

The tracking function lets you monitor what are known as tracking objects. Examples of monitored tracking objects are the link status of an interface or the reachability of a remote router or end device.

The device forwards status changes of the tracking objects to the registered applications, for example to the routing table or to a VRRP instance. The applications then react to the status changes:

- In the routing table, the device activates/deactivates the route linked to the tracking object.
- The VRRP instance linked to the tracking object reduces the priority of the virtual router so that a backup router takes over the role of the master.
- When the status of the tracking object changes, the device enables/disables the interface linked to the tracking object. The device displays the corresponding application in the [Advanced > Tracking > Applications](#) dialog.

If you set up the tracking objects in the [Advanced > Tracking > Configuration](#) dialog, then you can link applications with the tracking objects:

- You link static routes with a tracking object in the [Routing > Routing Table](#) dialog, *Track name* column.
- You link virtual routers with a tracking object in the [Routing > L3-Redundancy > VRRP > Tracking](#) dialog. Click the  button to open the *Create* window and select the tracking object from the *Track name* drop-down list.
- You link the interface status with a tracking object in the [Basic Settings > Port](#) dialog, *Track name* column.

The menu contains the following dialogs:

- [Tracking Configuration](#)
- [Tracking Applications](#)

7.5.1 Tracking Configuration

[Advanced > Tracking > Configuration]

In this dialog, you set up the tracking objects.

Table

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

Buttons



Add

Opens the [Create](#) window to add a table row.

- From the [Type](#) drop-down list, you select the type of the tracking object.
Possible values:
 - [i n t e r f a c e](#)
The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.
 - [l o g i c a l](#)
The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.
- In the [Track ID](#) field, you specify the identification number of the tracking object.
Possible values:
 - [1 . . 256](#)



Remove

Removes the selected table row.

Type

Specifies the type of the tracking object.

Possible values:

[i n t e r f a c e](#)

The device monitors the link status of its physical ports or of its link aggregation, LRE or VLAN router interface.

[l o g i c a l](#)

The device monitors tracking objects logically linked to each other and thus enables complex monitoring tasks.

Track ID

Specifies the identification number of the tracking object.

Possible values:

[1 . . 256](#)

This range is available to every type ([i n t e r f a c e](#), [p i n g](#) and [l o g i c a l](#)).

Track name

Displays the name of the tracking object made up of the values displayed in the *Type* and *Track ID* columns.

Active

Activates/deactivates the monitoring of the tracking object.

Possible values:

[marked](#)

Monitoring is active. The device monitors the tracking object.

[unmarked](#) (default setting)

Monitoring is inactive.

Description

Specifies the description.

Here you describe what the device uses the tracking object for.

Possible values:

Alphanumeric ASCII character string with 0..255 characters

Status

Displays the monitoring result of the tracking object.

Possible values:

[up](#)

The monitoring result is positive:

- The link status is active.

or

- The remote router or end device is reachable.

or

- The result of the logical link is *TRUE*.

[down](#)

The monitoring result is negative:

- The link status is inactive.

or

- The remote router or end device is not reachable.

or

- The result of the logical link is *FALSE*.

[not Ready](#)

The monitoring of the tracking object is inactive. You activate the monitoring in the *Active* column.

Changes

Displays the number of status changes since the tracking object has been activated.

Last changed

Displays the time of the last status change.

Send trap

Activates/deactivates the sending of an SNMP trap when someone activates or deactivates the tracking object.

Possible values:

`marked`

If someone activates or deactivates the tracking object in the *Active* column, then the device sends an SNMP trap.

`unmarked` (default setting)

The device does not send an SNMP trap.

Port

Specifies the interface to be monitored for tracking objects of the *interface* type.

Possible values:

`<interface number>`

Number of the physical ports or of the link aggregation, LRE or VLAN router interface.

`no Port`

No tracking object of the *interface* type.

Link up delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as positive. If the link has been active on the interface for longer than the period specified here, then the *Status* column displays the value *up*.

Possible values:

`0 . 255`

`-`

No tracking object of the *logical* type.

Link down delay [s]

Specifies the period in seconds after which the device evaluates the monitoring result as negative. If the link has been inactive on the interface for longer than the period specified here, then the *Status* column displays the value *down*.

Possible values:

`0 . 255`

`-`

No tracking object of the *interface* type.

If the link to every aggregated port is interrupted, then Link aggregation, LRE and VLAN router interfaces have a negative monitoring result.

If the link to every physical port and link-aggregation interface which is a member of the VLAN is interrupted, then a VLAN router interface has a negative monitoring result.

Logical operand A

Specifies the first operand of the logical link for tracking objects of the **Logical** type.

Possible values:

Tracking objects set up

–

No tracking object of the **Logical** type.

Logical operand B

Specifies the second operand of the logical link for tracking objects of the **Logical** type.

Possible values:

Tracking objects set up

–

No tracking object of the **Logical** type.

Operator

Links the tracking objects specified in the *Logical operand A* and *Logical operand B* fields.

Possible values:

and

Logical AND link

or

Logical OR link

–


No tracking object of the **Logical** type.

7.5.2 Tracking Applications

[Advanced > Tracking > Applications]

In this dialog, you see which applications are linked with the tracking objects.

The following applications can be linked with tracking objects:

- You link static routes with a tracking object in the [Routing > Routing Table](#) dialog, *Track name* column.
- You link virtual routers with a tracking object in the [Routing > L3-Redundancy > VRRP > Tracking](#) dialog. Click the  button to open the *Create* window and select the tracking object from the *Track name* drop-down list.
- You link the interface status with a tracking object in the [Basic Settings > Port](#) dialog, *Track name* column.

Table

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

Type

Displays the type of the tracking object.

Track ID

Displays the identification number of the tracking object.

Application

Displays the name of the application that is linked with the tracking object.

Possible values:

Tracking objects of the [logical](#) type

Static routes

Virtual router of a VRRP instance

Interface status

Track name

Displays the name of the tracking object made up of the values displayed in the [Type](#) and [Track ID](#) columns.

7.6 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 | 217 |
| 802.1X | 91, 136 |
| A | |
| Access control | 136 |
| Access control lists | 166 |
| Access restriction | 116 |
| ACL | 166 |
| Address conflict detection | 303 |
| Aging time | 177 |
| Alarm | 292 |
| ARP | 303 |
| ARP table | 70, 307 |
| Audit trail | 368 |
| Authentication history | 149 |
| Authentication list | 91 |
| Auto disable | 132, 133, 239, 333, 334, 340, 356 |
| B | |
| Bridge | 236 |
| C | |
| CA (Certification Authority) | 96, 313, 322 |
| Cable diagnosis | 328 |
| Certificate | 21, 46, 96, 113, 114, 282, 313, 322 |
| Certificate Revocation List (CRL) | 96, 313, 322 |
| Certification Authority (CA) | 96, 313, 322 |
| CLI | 120 |
| Command line interface | 120 |
| Community names | 122 |
| Configuration check | 301 |
| Configuration profile | 16, 42 |
| Counter reset | 69 |
| CRL (Certificate Revocation List) | 96, 313, 322 |
| D | |
| Daylight saving time | 74 |
| Default gateway | 375 |
| Device software | 38 |
| Device software backup | 38 |
| Device status | 19, 272 |
| DHCP L2 Relay | 378 |
| DHCP server | 369 |
| DHCPv6 L2 Relay | 378 |
| Digital certificate | 21, 46, 96, 114, 282, 313, 322 |
| DNS | 383 |
| DNS cache | 384 |
| DNS client | 384 |
| Domain name system | 383 |
| DoS | 162 |
| DSCP | 218 |
| Duplicate Address Detection | 34 |

| | |
|----------------------------------|---|
| E | |
| EAPOL | 147 |
| Egress rate limiter | 180 |
| Email notification | 71, 311 |
| Encryption | 42 |
| ENVM | 41, 47, 49, 54, 365 |
| Ethernet module | 275, 287, 289 |
| Ethernet modules | 273 |
| Event severity | 316, 363 |
| External memory | 22, 41, 47, 49, 54, 274, 280, 287, 288, 365 |
| F | |
| FAQ | 415 |
| FDB (MAC address table) | 70, 183 |
| Filter MAC addresses | 183 |
| Fingerprint | 110, 114 |
| Flash memory | 41, 300 |
| Flow control | 177 |
| G | |
| GARP | 209 |
| GMRP | 210 |
| Guards | 246 |
| GVRP | 212 |
| H | |
| Hardware clock | 73 |
| Hardware state | 300 |
| HiDiscovery | 27, 281, 368 |
| Host key | 110 |
| HTML | 299, 367 |
| HTTP | 111 |
| HTTP server | 279 |
| HTTPS | 112 |
| I | |
| IAS | 91, 151 |
| IEC61850-MMS | 282, 391 |
| IEEE 802.1X | 91 |
| IGMP snooping | 70, 185 |
| Industrial HiVision | 9, 105 |
| Ingress filtering | 227 |
| Ingress rate limiter | 180 |
| Integrated authentication server | 91, 151 |
| IP access restriction | 116 |
| IP address conflict detection | 303 |
| IP DSCP mapping | 218 |
| IPv4 rule | 167 |

| | |
|---|--------------|
| L | |
| L2 Relay (DHCP) | 378 |
| LDAP | 91 |
| Link aggregation | 249 |
| Link backup | 255 |
| Link status | 273, 287 |
| LLDP | 346 |
| Load/save | 42 |
| Log file | 69, 71, 367 |
| Login banner | 121, 124 |
| Loop protection | 288 |
| Loops | 235 |
| M | |
| MAC flood | 131 |
| MAC rule | 171 |
| MAC spoof | 133 |
| MAC address table (forwarding database) | 70, 183 |
| Management access | 27, 32, 116 |
| Management access statistics | 70 |
| Management VLAN | 27 |
| Manufacturing message specification | 391 |
| Media redundancy protocol | 231 |
| MMRP | 201 |
| MMS | 391 |
| Modbus TCP | 282, 394 |
| Modules | 273 |
| MRP | 231 |
| MRP-IEEE | 199 |
| MVRP | 206 |
| N | |
| Network load | 62 |
| NVM | 16, 41, 47 |
| O | |
| Out-of-band management port | 36 |
| P | |
| Password | 86, 278 |
| Password length | 86, 278 |
| Persistent log file | 71 |
| Persistent logging | 364 |
| PoE | 63 |
| Port clients | 145 |
| Port configuration | 139, 215 |
| Port mirroring | 344 |
| Port monitor | 340 |
| Port priority | 215 |
| Port security | 131 |
| Port statistics | 70, 147 |
| Port VLAN | 226 |
| Port-based access control | 136 |
| Power over Ethernet | 63 |
| Power supply | 21, 274, 288 |
| Pre-Login banner | 124 |
| Priority queue | 214 |

| | |
|-----------------------------------|--|
| Q | |
| Queue management | 220 |
| Queues | 214 |
| R | |
| RADIUS | 91, 152 |
| RAM | 46 |
| RAM self-test | 309 |
| Rate limiter | 180 |
| Reboot | 69 |
| Relay (DHCP) | 378 |
| Request interval | 79 |
| Ring redundancy | 274, 288 |
| Ring structure | 231 |
| Ring/Network coupling | 264 |
| RNC | 264 |
| Root bridge | 236 |
| RSTP | 235, 236 |
| S | |
| Secure Boot | 40, 282 |
| Secure Shell (SSH) | 107 |
| Security status | 20, 277 |
| Self-test | 309 |
| Serial interface | 280 |
| Settings | 42 |
| Severity | 316, 363 |
| SFP module | 327 |
| Signal contact | 20, 284 |
| SNMP server | 105, 280 |
| SNMP traps | 60, 65, 133, 236, 252, 272, 277, 286, 292, 305, 333, 404 |
| SNMPv1/v2 | 122 |
| SNTP | 77 |
| SNTP client | 78 |
| SNTP server | 82 |
| Software backup | 38 |
| Software update | 38 |
| Spanning tree protocol | 235 |
| SSH server | 107 |
| Sub Ring | 259 |
| Support information | 360 |
| Support information (ZIP archive) | 363 |
| Syslog | 321 |
| System information | 299 |
| System log | 367 |
| System monitor | 309 |
| System time | 73 |

| | |
|---|--|
| T | |
| Technical questions | 415 |
| Telnet server | 106, 279 |
| Temperature | 21, 273, 287 |
| Threshold values network load | 180 |
| Topology discovery | 351 |
| Tracking | 401 |
| Training courses | 415 |
| Trap destination | 296 |
| Traps | 60, 65, 133, 236, 252, 272, 277, 286, 292, 305, 333, 404 |
| Trust mode | 215 |
| Twisted-pair | 328 |
| U | |
| Unaware mode | 177 |
| Unsigned device software (allow upload) | 40 |
| Uptime | 21, 300 |
| USB network interface | 36 |
| User administration | 85 |
| Utilization | 62 |
| V | |
| Virtual local area network | 221 |
| VLAN | 29, 33, 221, 357 |
| VLAN configuration | 223 |
| VLAN ports | 226 |
| VLAN-unaware mode | 177 |
| W | |
| Watchdog | 42, 51 |
| Web server | 111, 112 |
| Z | |
| ZIP archive with support information | 363 |

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 hirschmann-support.belden.com. This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

Training offers you an introduction to the basics, product briefing and user training with certification. You find the training courses on technology and products currently available at www.belden.com/solutions/customer-innovation-center.

Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

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 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Readability | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Understandability | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Examples | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Structure | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Comprehensive | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Graphics | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Drawings | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Tables | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

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





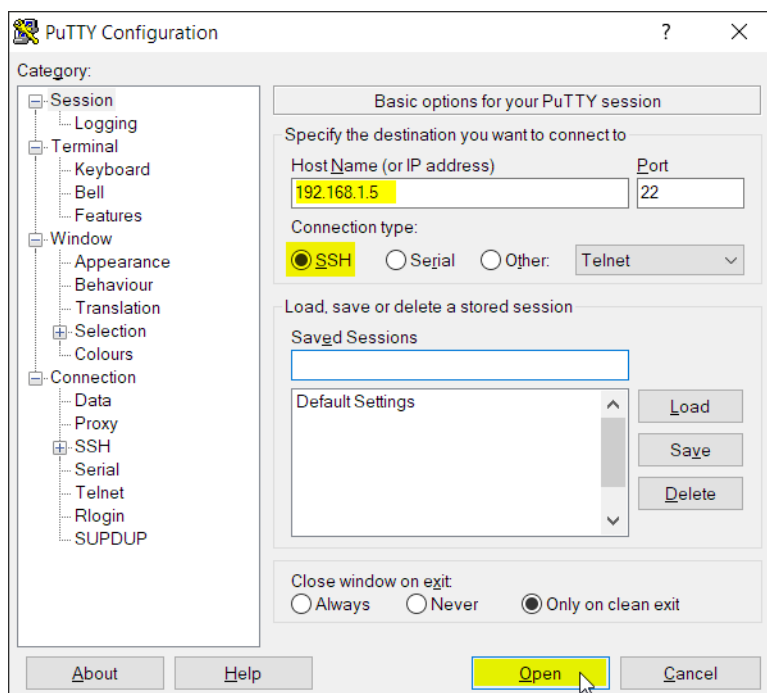


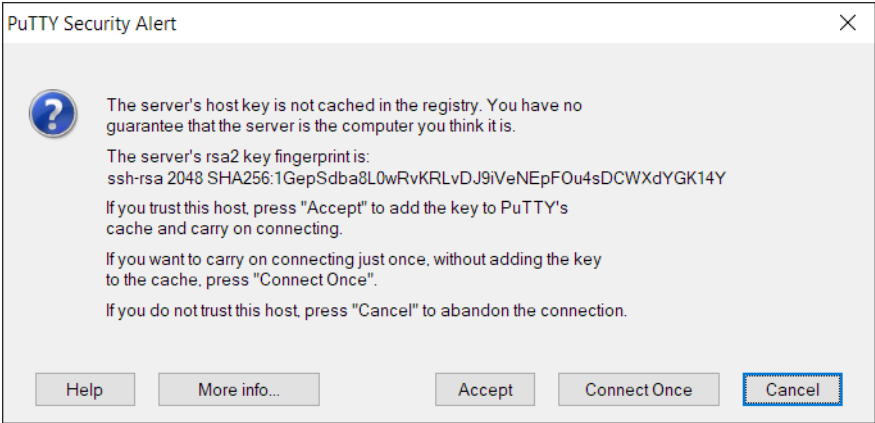


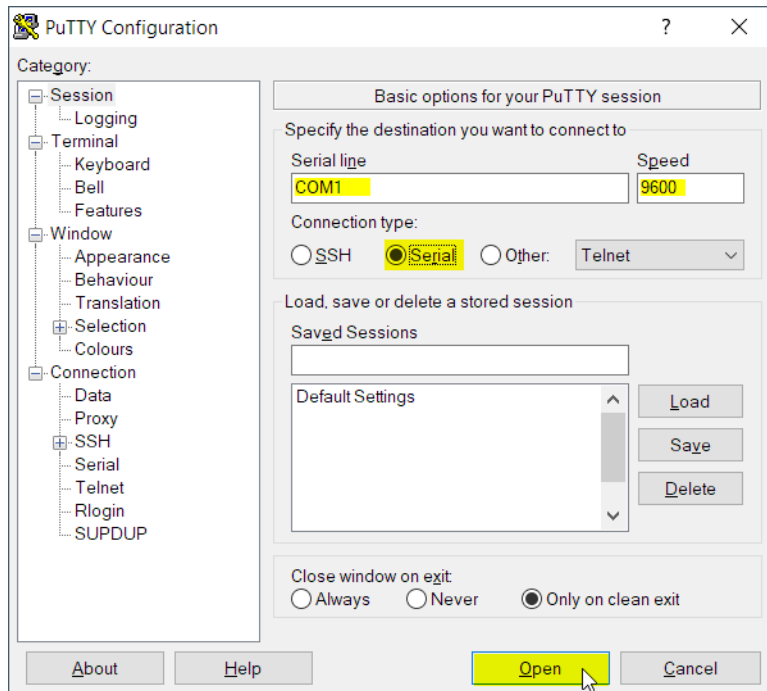


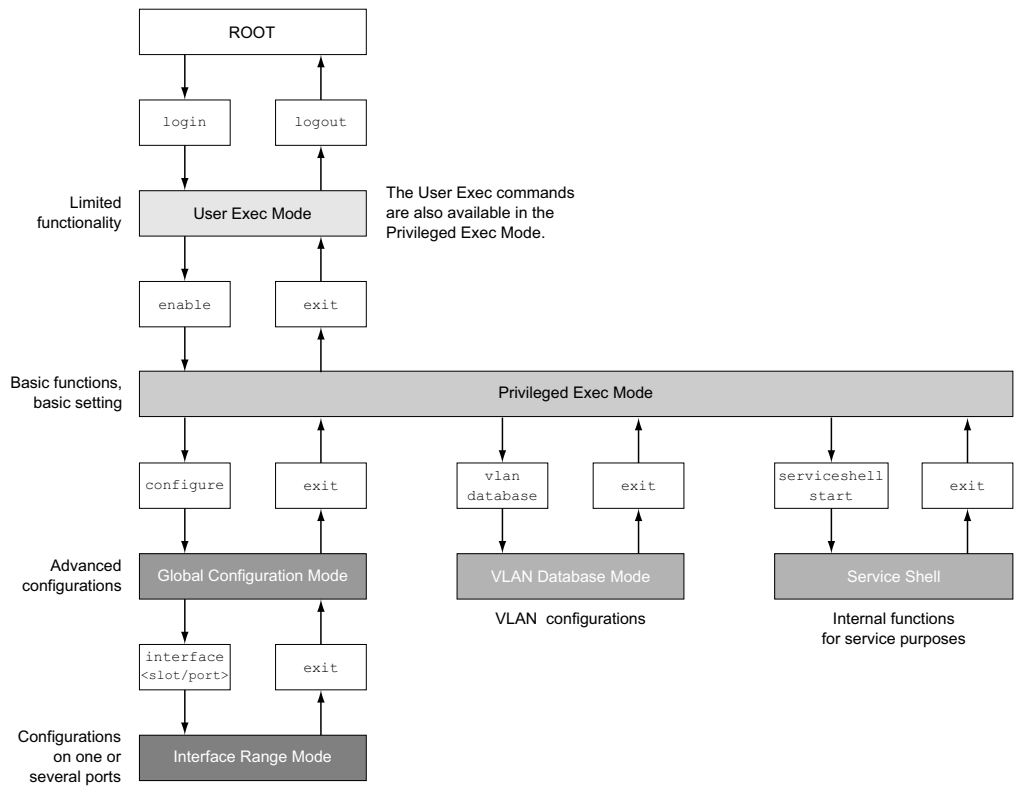














A series of horizontal lines for writing, consisting of 20 parallel black lines spaced evenly down the page.





| | | | |
|---------|-----------------------------------|-------------------|---------|
| 0 | Net ID - 7 bits | Host ID - 24 bits | Class A |
| 1 0 | Net ID - 14 bits | Host ID - 16 bits | Class B |
| 1 1 0 | Net ID - 21 bits | Host ID - 8 bits | Class C |
| 1 1 1 0 | Multicast Group ID - 28 bits | | Class D |
| 1 1 1 1 | reserved for future use - 28 bits | | Class E |

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000



Decimal notation

129.218.65.17

└─── 128 < 129 191 > Class B

Binary notation

10000001.11011010.01000001.00010001

└─── Subnetwork 1
└─── Network address

Decimal notation

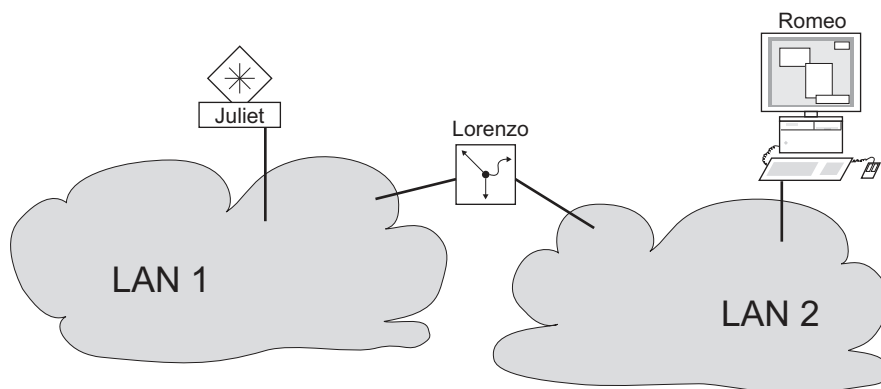
129.218.129.17

└─── 128 < 129 191 > Class B

Binary notation

10000001.11011010.10000001.00010001

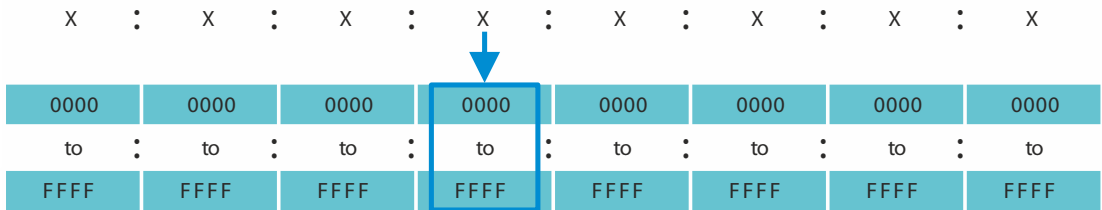
└─── Subnetwork 2
└─── Network address



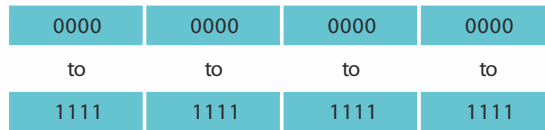
| IP address,
decimal | Network mask,
decimal | IP address,
binary |
|------------------------|--------------------------|-------------------------------------|
| 192.168.112.1 | 255.255.255.128 | 11000000 10101000 01110000 00000001 |
| 192.168.112.127 | | 11000000 10101000 01110000 01111111 |
| | | ----- 25 mask bits ----- |

CIDR notation: 192.168.112.0/25

└─── Mask bits



in binary



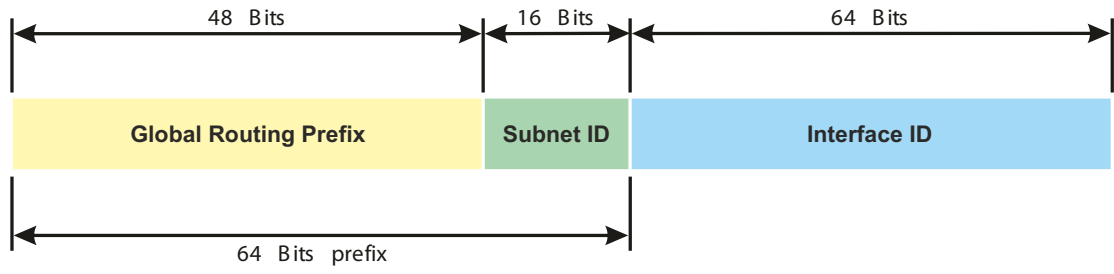
64 bits prefix length

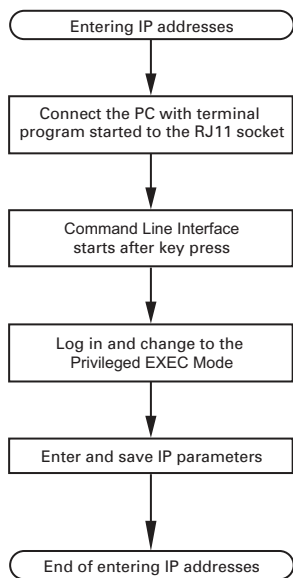
64 bits interface ID

Address example: 2009:0CB8:0000:0004::10 / 64

2009:0CB8:0000:0004


0000:0000:0000:0010





```
NOTE: Enter '?' for Command Help. Command help displays all opt  
that are valid for the particular mode.  
For the syntax of a particular command form, please  
consult the documentation.
```

```
! ( )>
```



```
NOTE: Enter '?' for Command Help. Command help displays all opt
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.
```

```
! ( ) > █
```


| Id | MAC Address | Writable | IP Address | Net Mask | Default Gateway | Product | Name |
|----|-------------------|-------------------------------------|----------------|---------------|-----------------|---------|------|
| 1 | 00:80:63:A4:CC:00 | <input checked="" type="checkbox"/> | 10.115.0.76 | 255.255.224.0 | 10.115.0.3 | | |
| 2 | 00:80:63:C0:50:00 | <input type="checkbox"/> | 10.115.0.33 | 255.255.224.0 | 10.115.0.3 | | |
| 3 | 00:80:63:A3:40:00 | <input type="checkbox"/> | 10.115.0.70 | 255.255.224.0 | 10.115.0.3 | | |
| 4 | 00:80:63:98:14:00 | <input type="checkbox"/> | 10.115.0.17 | 255.255.224.0 | 10.115.0.3 | | |
| 5 | 00:80:63:9E:E4:00 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | | |
| 6 | 00:80:63:46:00:06 | <input checked="" type="checkbox"/> | 192.168.2.181 | 255.255.255.0 | 192.168.2.1 | | |
| 7 | 00:80:63:A3:40:40 | <input type="checkbox"/> | 10.115.0.59 | 255.255.224.0 | 10.115.0.3 | | |
| 8 | 00:80:63:A4:CC:40 | <input type="checkbox"/> | 10.115.0.81 | 255.255.224.0 | 10.115.0.3 | | |
| 9 | 00:80:63:6E:38:4E | <input checked="" type="checkbox"/> | 192.168.2.174 | 255.255.255.0 | 192.168.2.1 | | |
| 10 | 00:80:63:18:2A:61 | <input checked="" type="checkbox"/> | 192.168.2.170 | 255.255.255.0 | 192.168.2.1 | | |
| 11 | 00:80:63:A3:40:80 | <input type="checkbox"/> | 10.115.0.66 | 255.255.224.0 | 10.115.0.3 | | |
| 12 | 00:80:63:A4:CC:80 | <input type="checkbox"/> | 10.115.0.80 | 255.255.224.0 | 10.115.0.3 | | |
| 13 | 00:80:63:61:AC:81 | <input checked="" type="checkbox"/> | 192.168.2.176 | 255.255.255.0 | 192.168.2.1 | | |
| 14 | 00:80:63:98:10:95 | <input type="checkbox"/> | 10.115.0.22 | 255.255.224.0 | 10.115.0.3 | | |
| 15 | 00:80:63:61:AC:AB | <input checked="" type="checkbox"/> | 192.168.2.40 | 255.255.255.0 | 192.168.2.1 | | |
| 16 | 00:80:63:3B:5C:BD | <input checked="" type="checkbox"/> | 192.168.2.178 | 255.255.255.0 | 192.168.2.1 | | |
| 17 | 00:80:63:A3:40:C0 | <input type="checkbox"/> | 10.115.0.72 | 255.255.224.0 | 10.115.0.3 | | |
| 18 | 00:80:63:8F:2C:BE | <input type="checkbox"/> | 10.115.0.40 | 255.255.224.0 | 10.115.0.3 | | |
| 19 | 00:80:63:88:38:EC | <input checked="" type="checkbox"/> | 192.168.110.92 | 255.255.255.0 | 0.0.0.0 | | |
| 20 | 00:80:63:9B:11:00 | <input type="checkbox"/> | 10.115.0.35 | 255.255.224.0 | 10.115.0.3 | | |
| 21 | 00:80:63:A4:CD:00 | <input type="checkbox"/> | 10.115.0.77 | 255.255.224.0 | 10.115.0.3 | | |
| 22 | 00:80:63:99:41:08 | <input type="checkbox"/> | 10.115.0.13 | 255.255.224.0 | 10.115.0.3 | | |
| 23 | 00:80:63:17:35:08 | <input checked="" type="checkbox"/> | 192.168.2.164 | 255.255.255.0 | 192.168.2.1 | | |
| 24 | 00:80:63:44:19:2E | <input checked="" type="checkbox"/> | 10.115.5.130 | 255.255.224.0 | 10.115.0.3 | | |

Properties

MAC Address: 00:80:63:A3:40:00

Name: Power Unit 1 Switch 2

IP Configuration

IP Address: 10 . 115 . 0 . 70 Set Default ()

Net Mask: 255 . 255 . 224 . 0 Set Default ()

Default Gateway: 10 . 115 . 0 . 3 Set Default ()

Save As Default

OK Cancel





⌘+







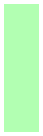




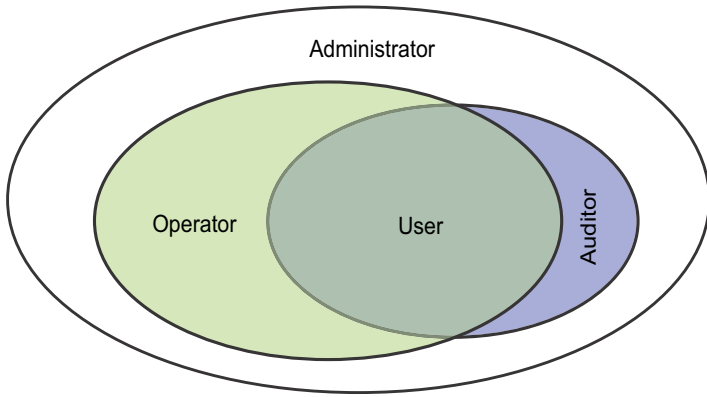




B+











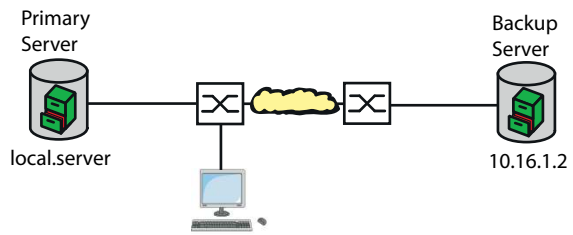


⌘+





0
x



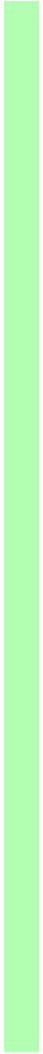




+

+

+









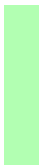




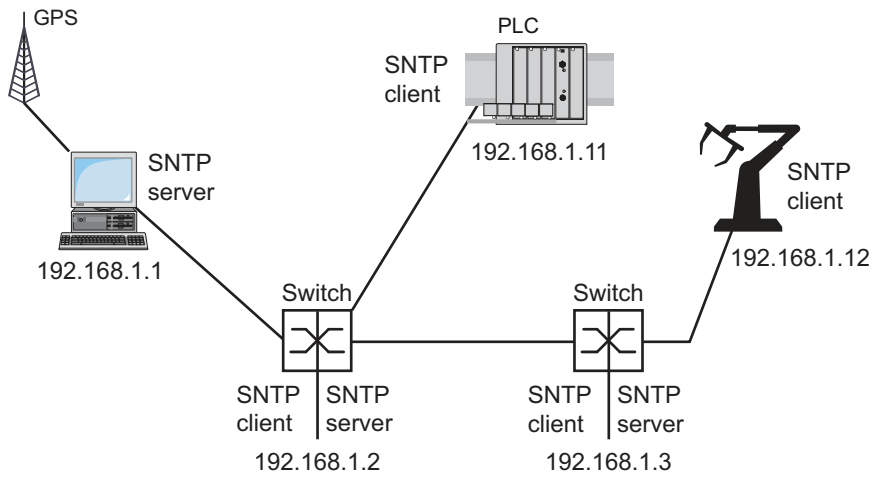




- [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

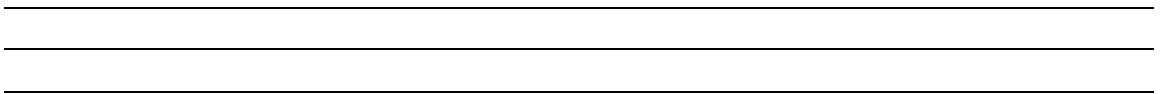








⌘+

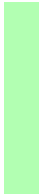


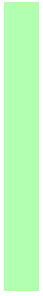




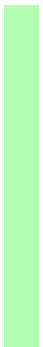








≡













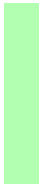






≡

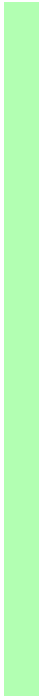








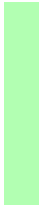








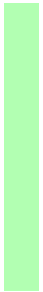




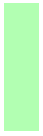
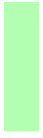














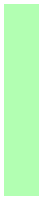
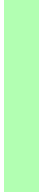


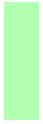
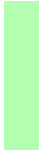
田+

田+













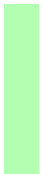
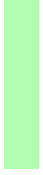
B+



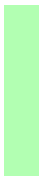
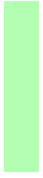
















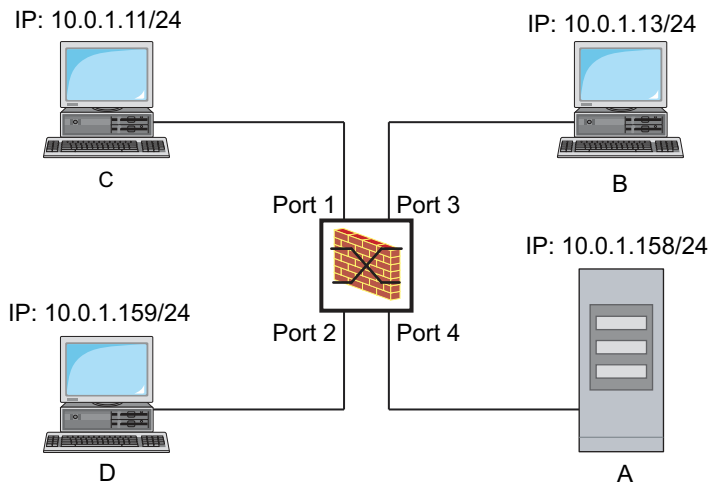


\mathbb{E}^+

+

\mathbb{E}^x

✓





β^+

+

β^+

✓







⌘+











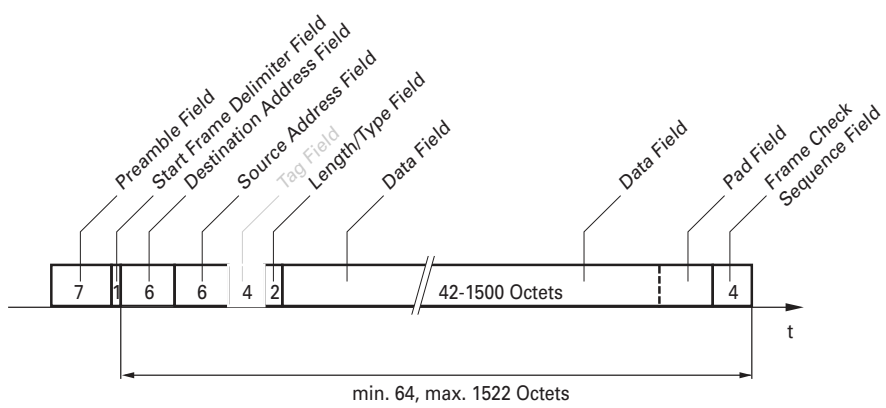


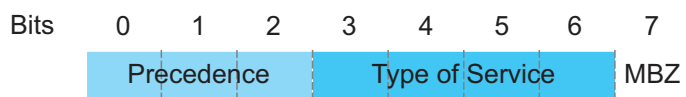
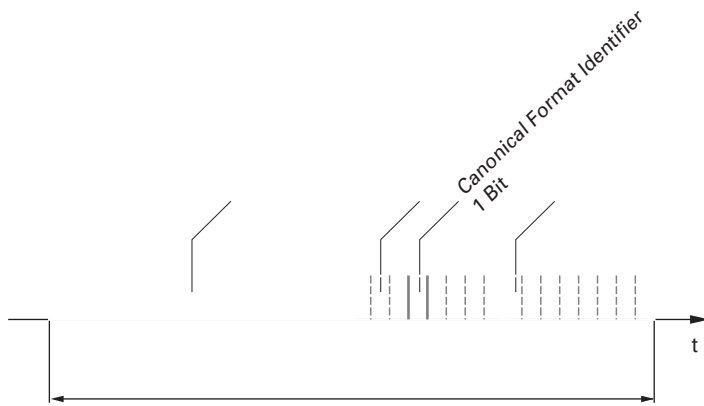








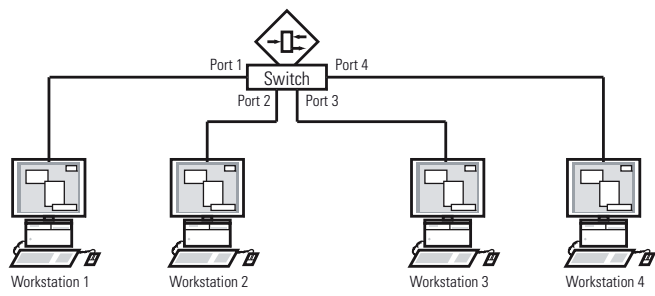














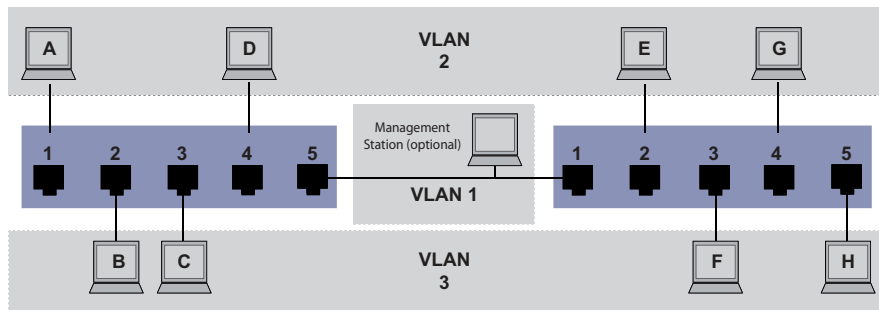




B+













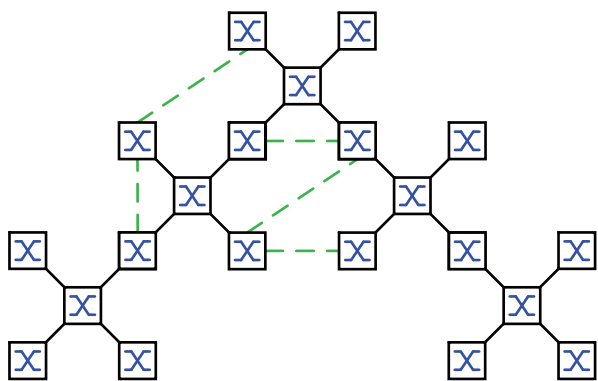
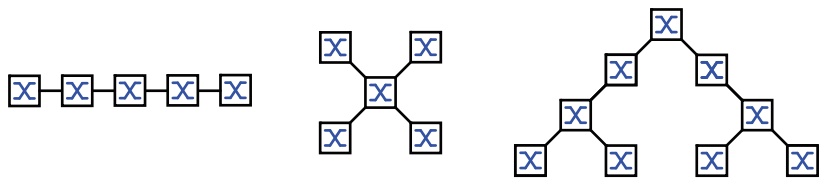


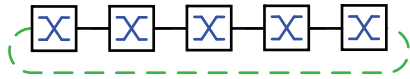
B+

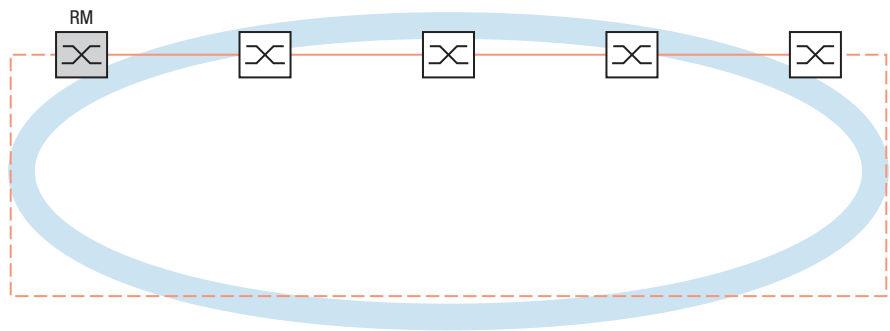
B+



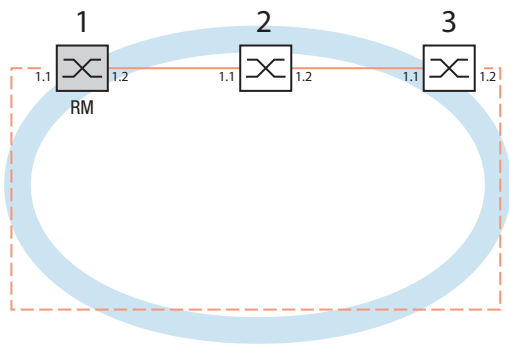






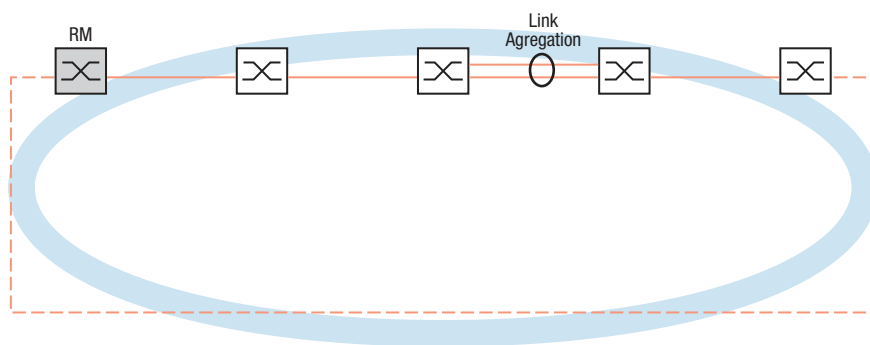


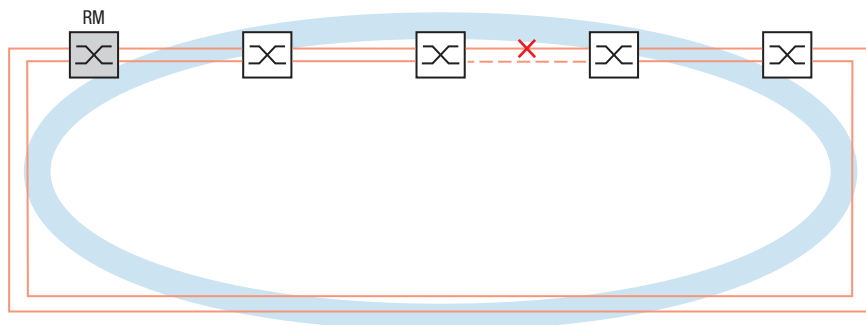
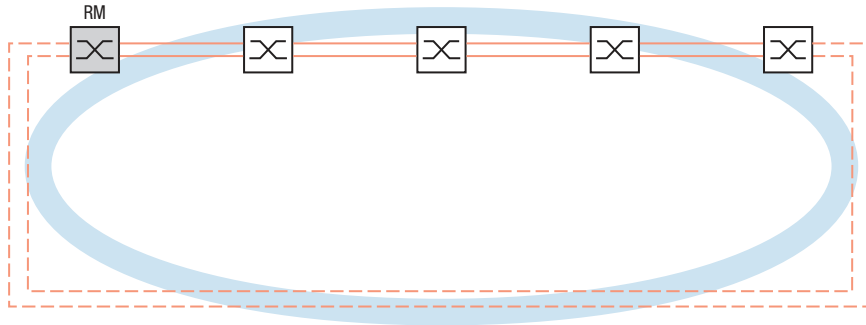


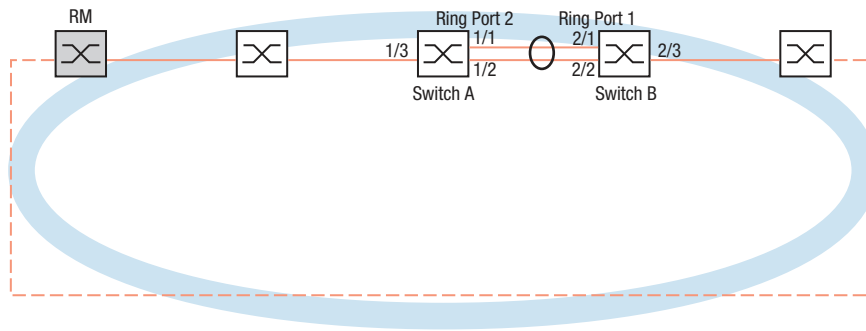










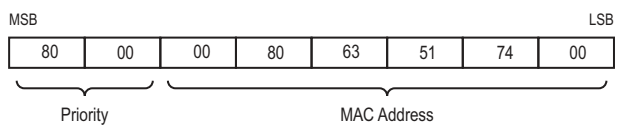


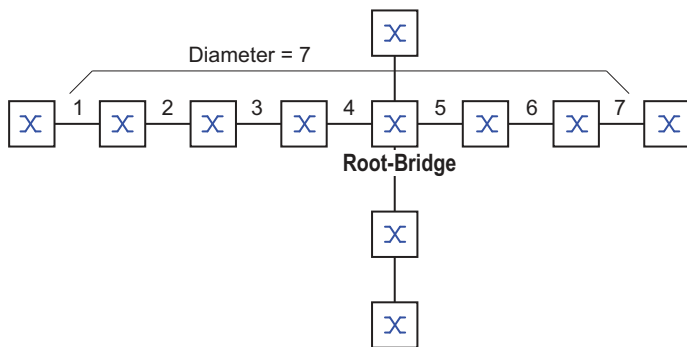
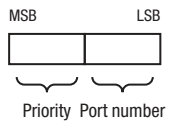
+



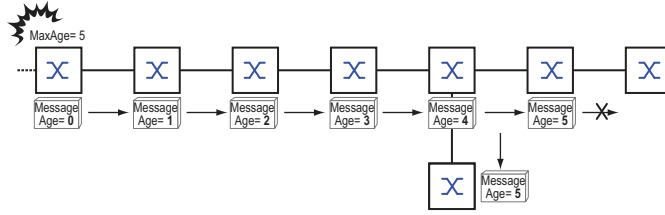


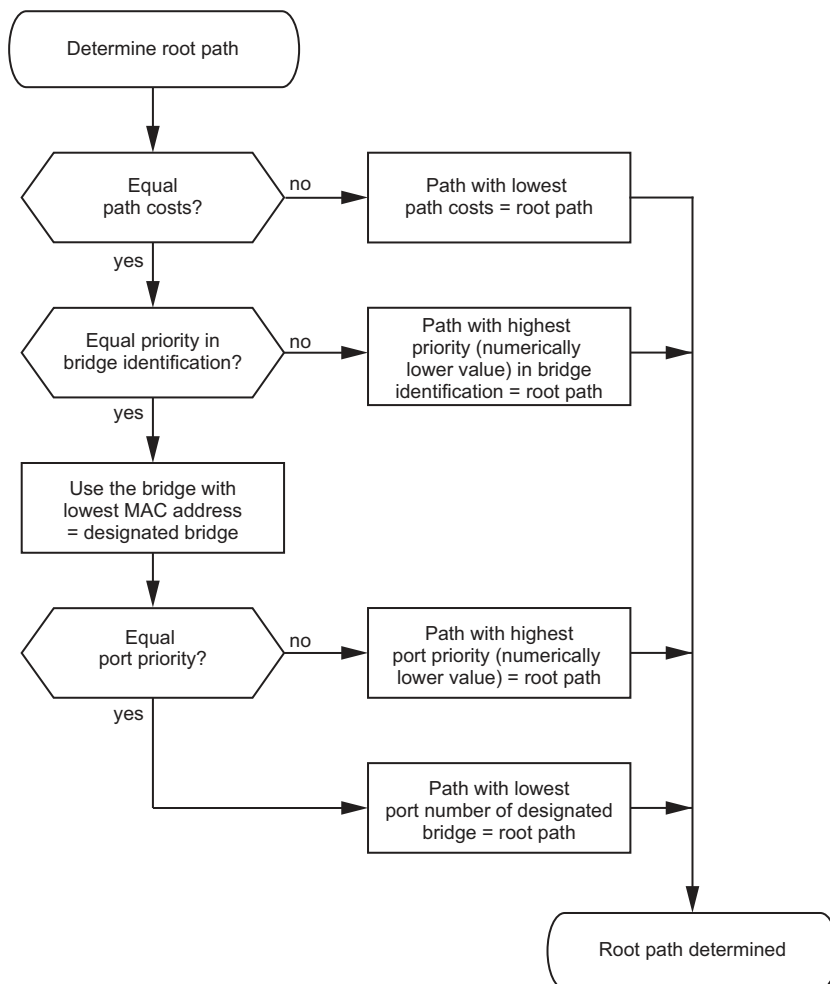


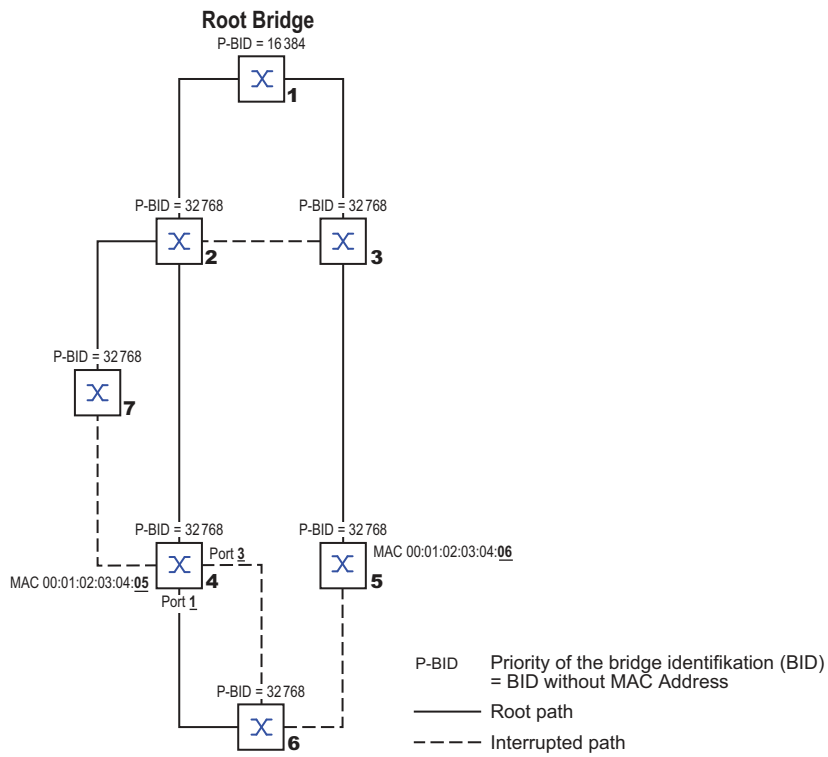


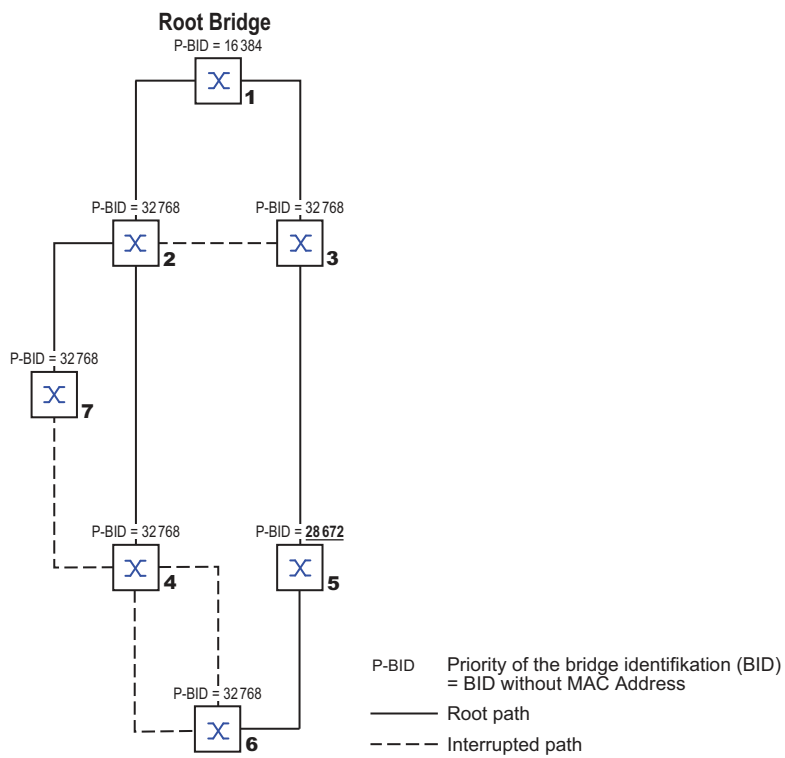


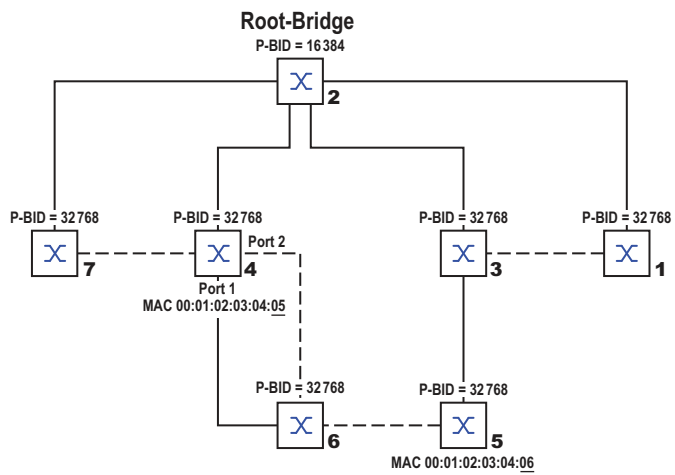
Root-Bridge







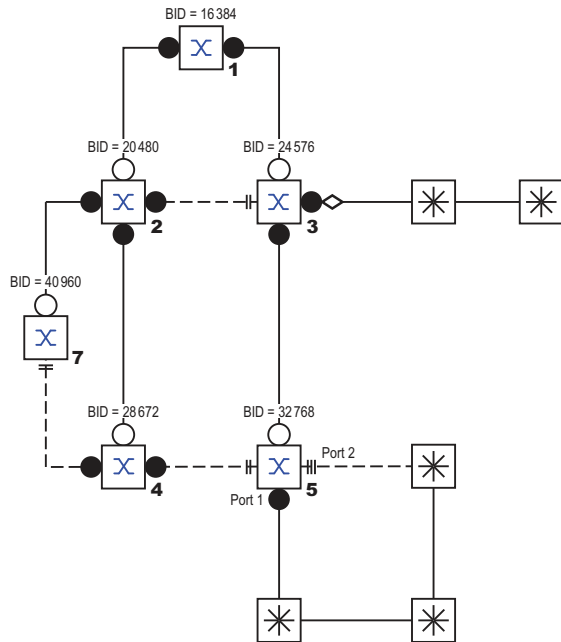




P-BID Priority of the bridge identification (BID)
= BID without MAC Address

—— Root path

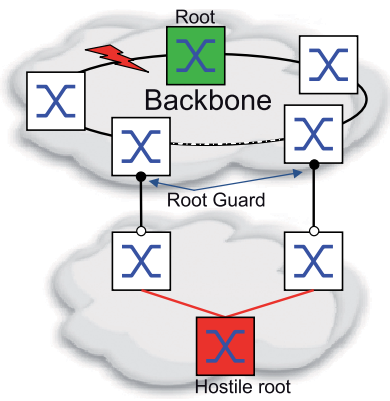
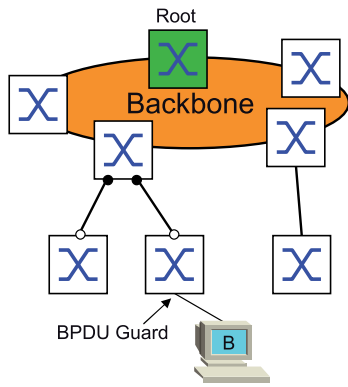
----- Interrupted path

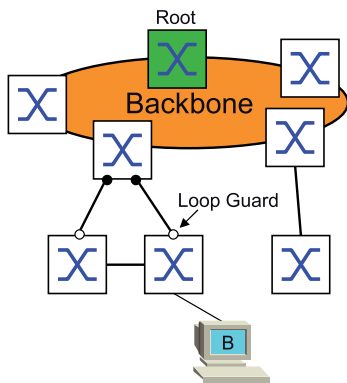
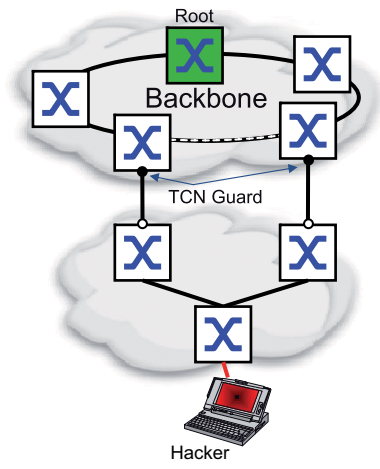


- P-BID Priority of the bridge identification (BID)
= BID without MAC Address
- Root path
- - - Interrupted path
- Root port
- Designated port
- || Alternate port
- ||| Backup port
- ◆ Edge port



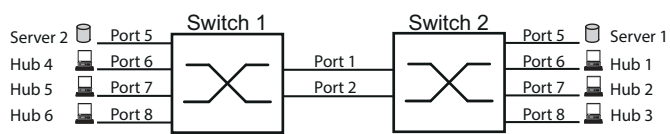








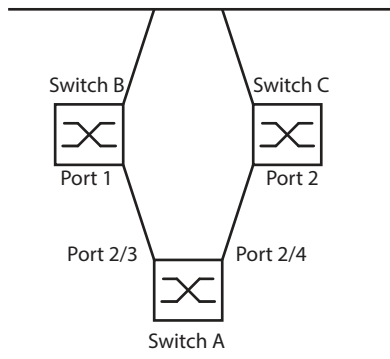






B+

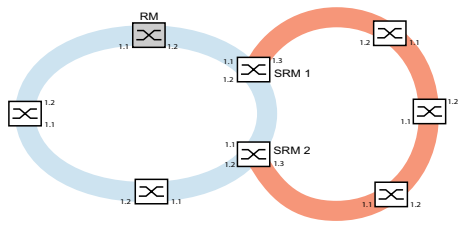


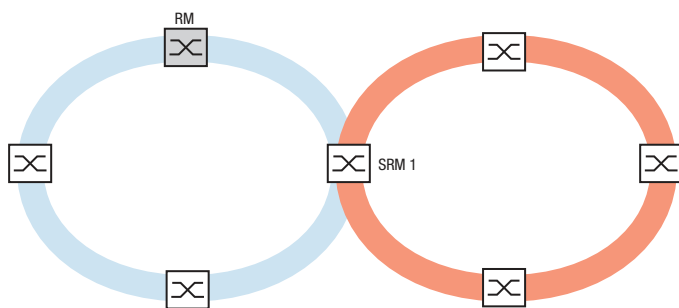
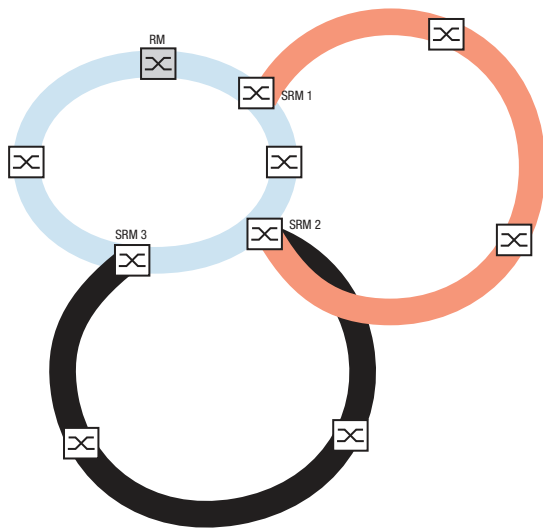
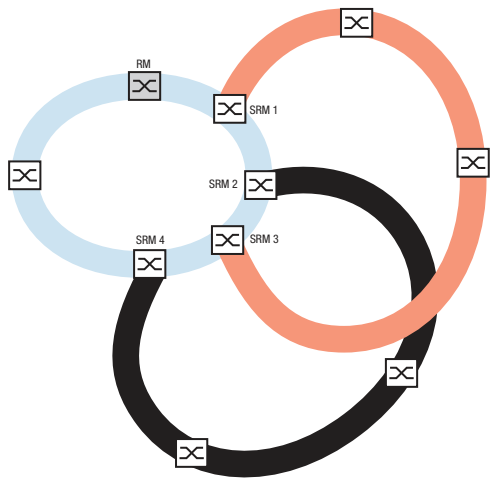


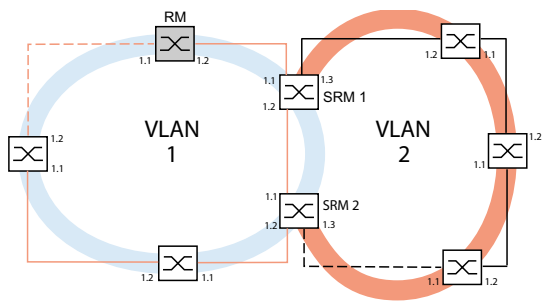
+



| |
|--|
| |
| |
| |





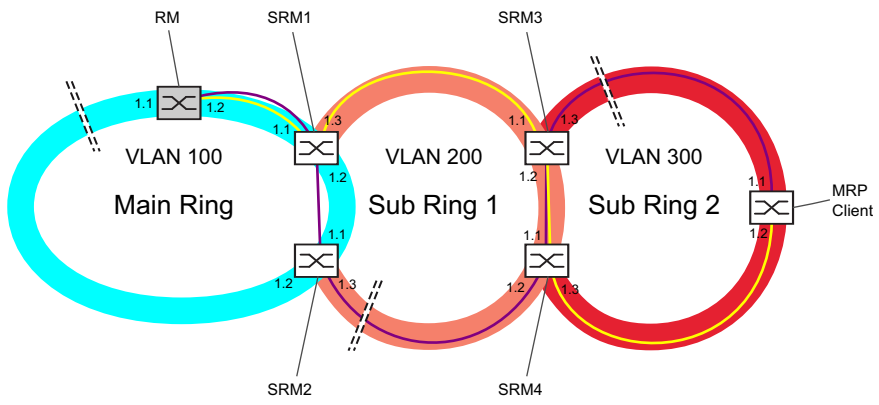






+







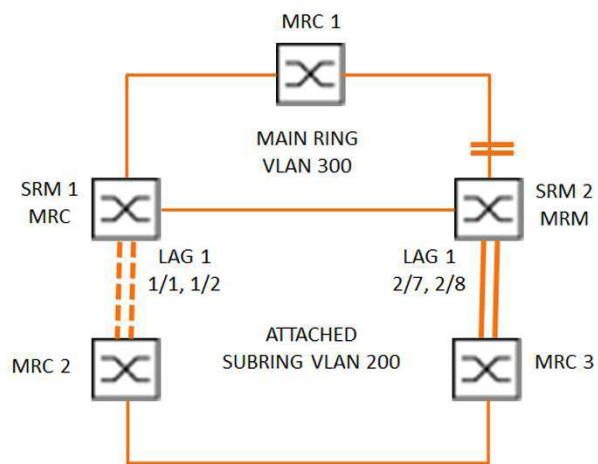


+

✓

✓

✓



1

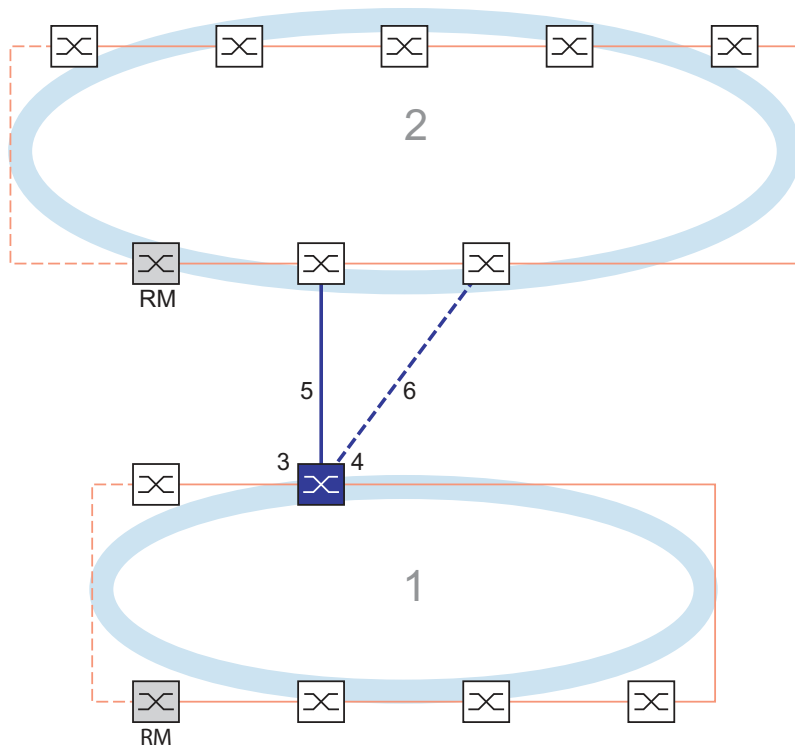
2

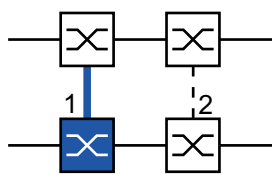
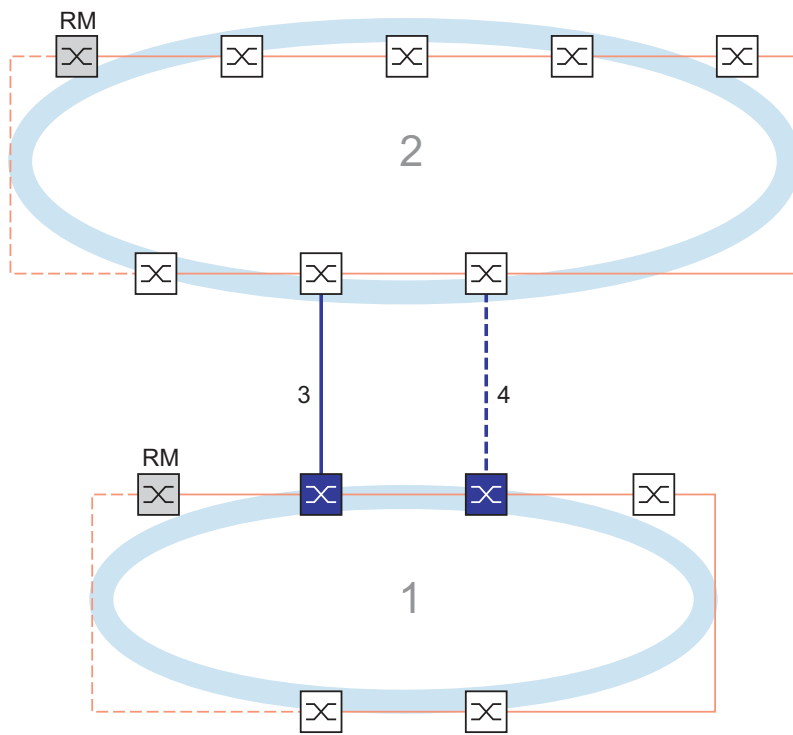
3

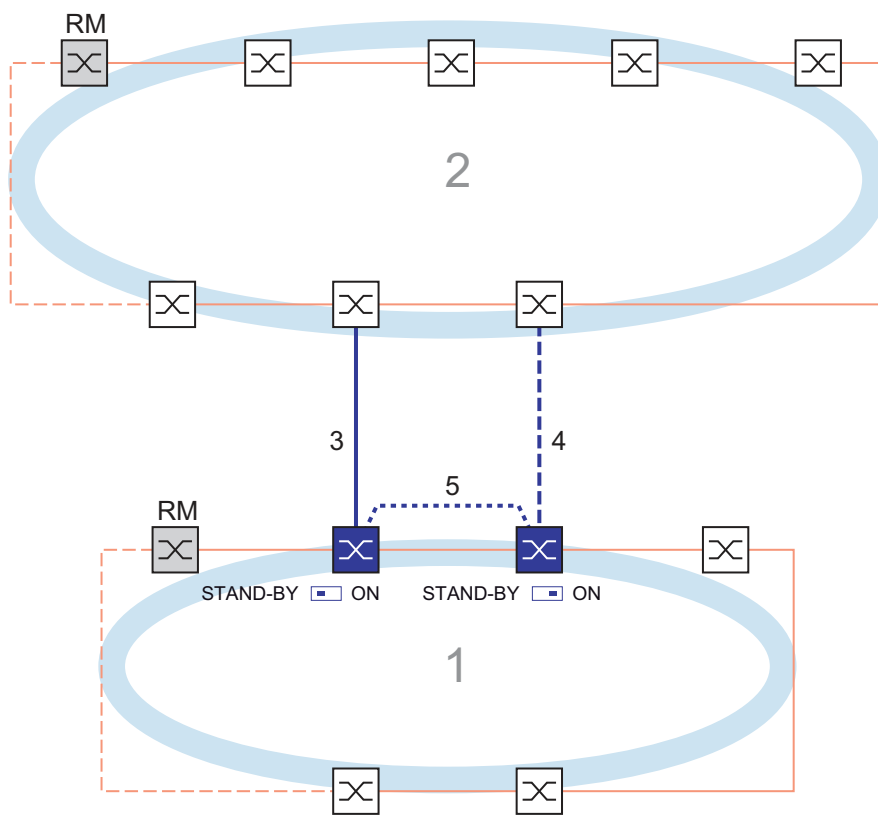
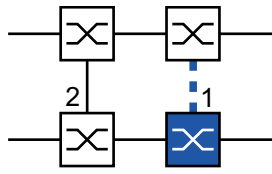


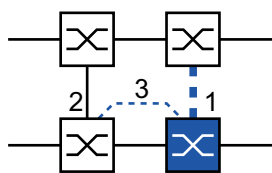
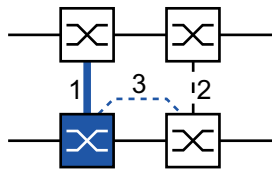




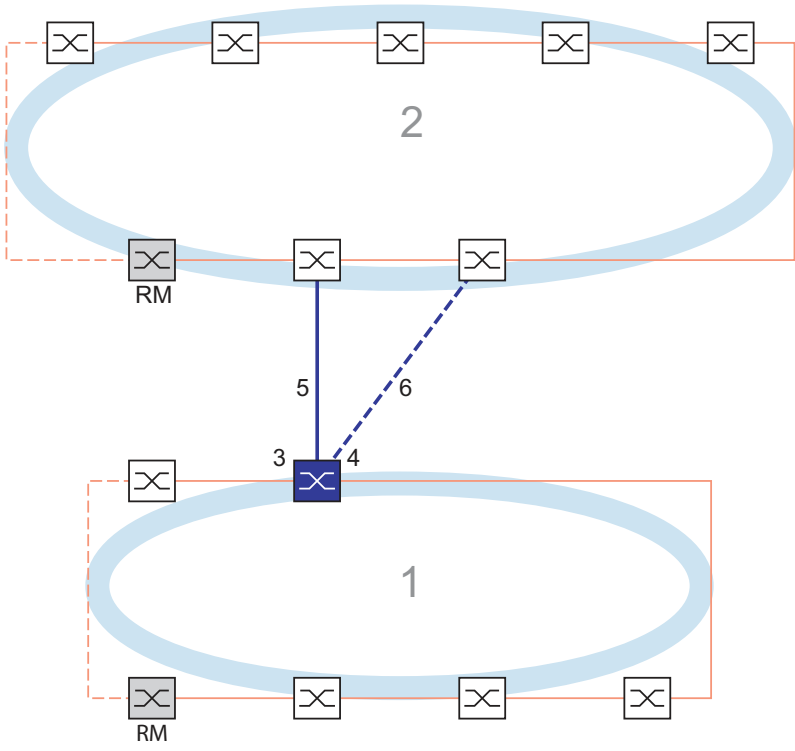


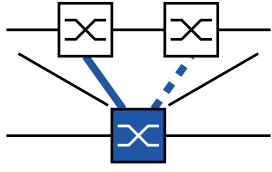




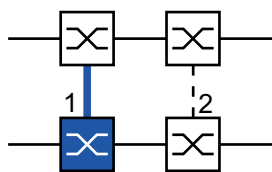
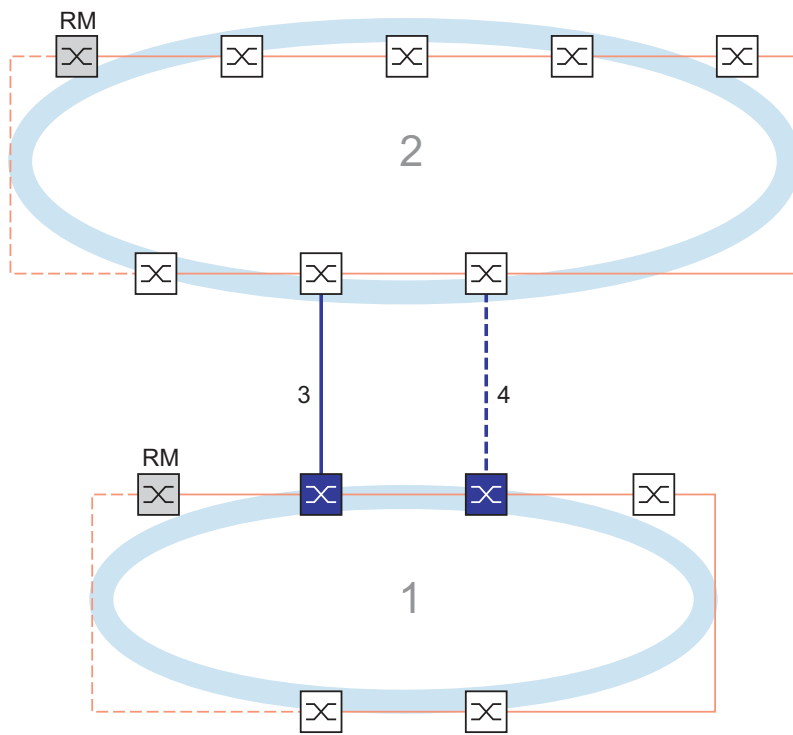




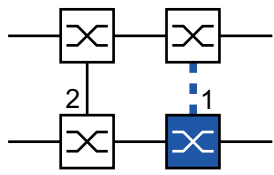


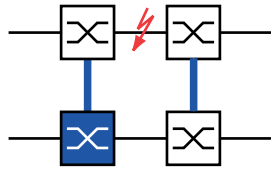


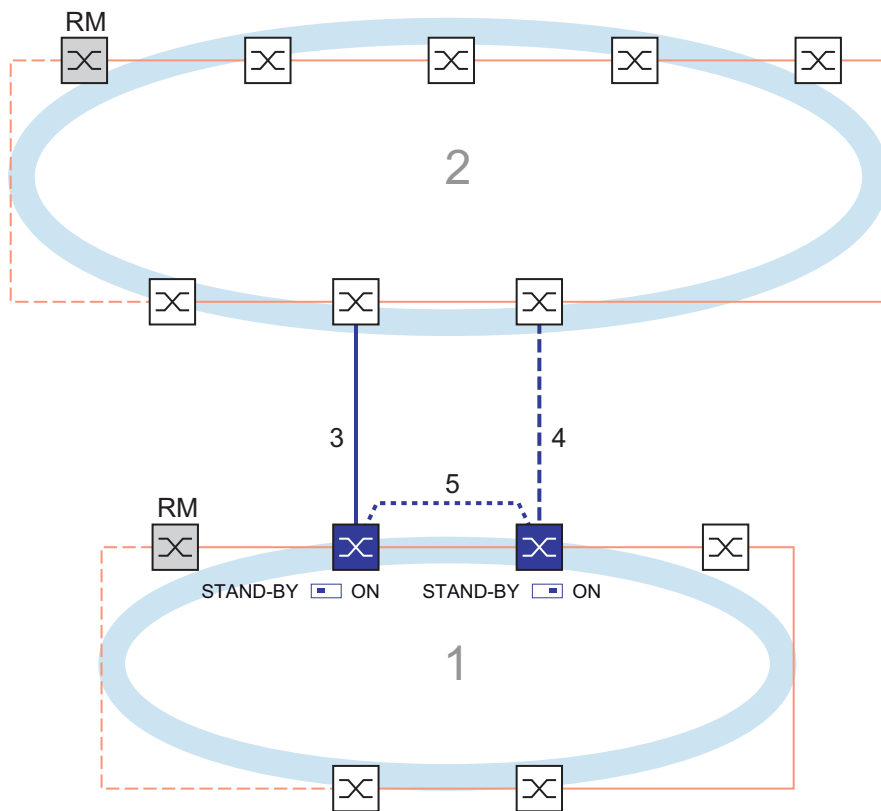


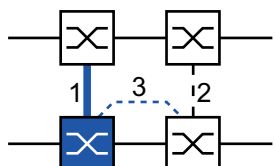


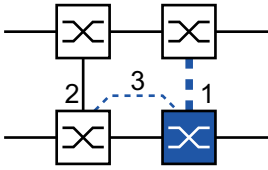




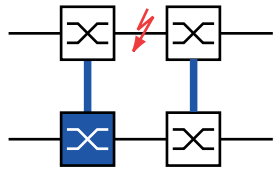


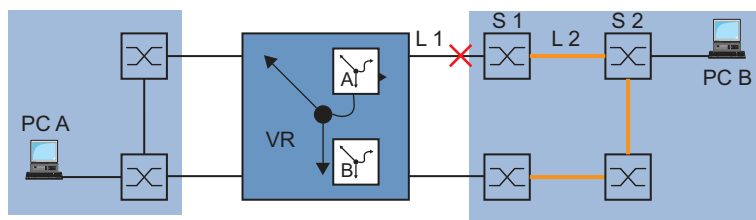








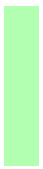






+









A series of 20 horizontal black lines, evenly spaced, providing a template for writing or drawing.



B+































A series of horizontal lines for writing, organized into four groups of four lines each, with a larger gap between the second and third groups.

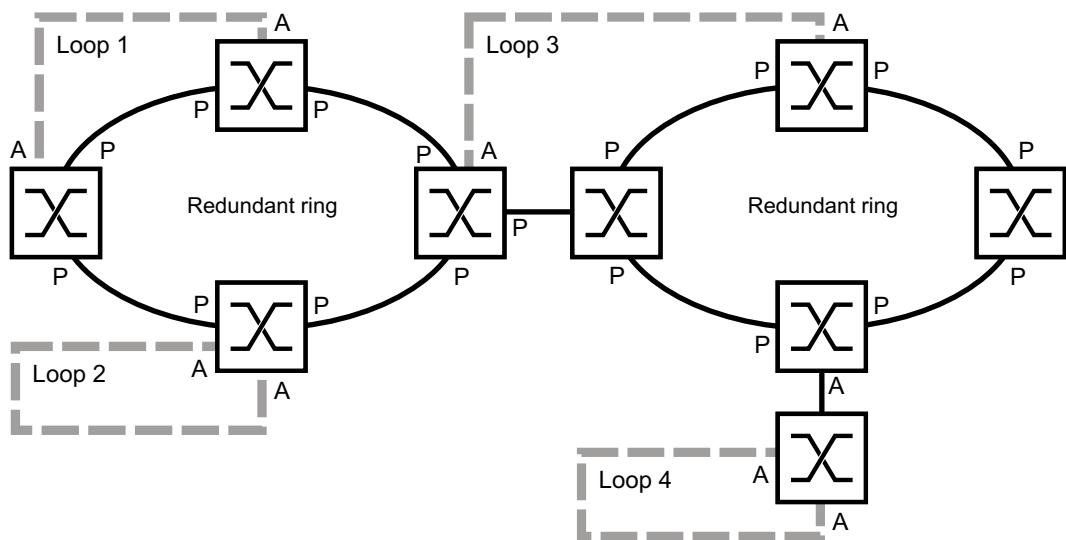








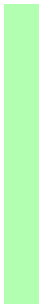














⊞
+



⊞
+







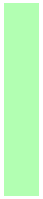
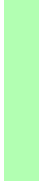




⌘+

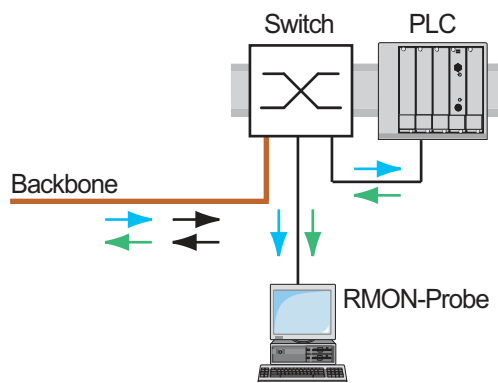




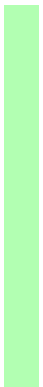




















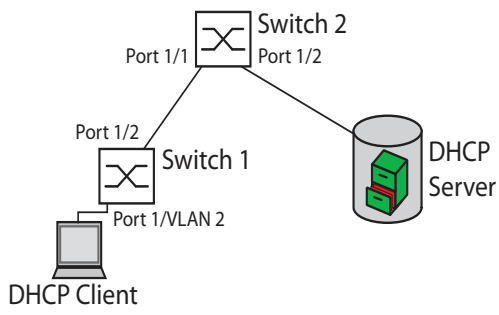
⌘ +



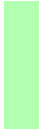


⌘+











+

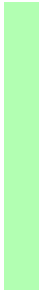


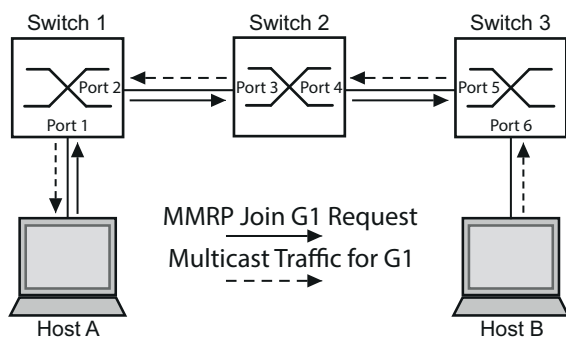


B+

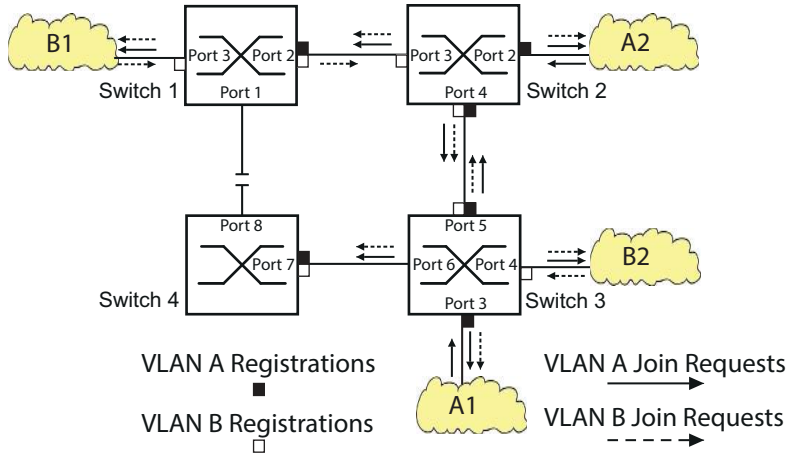




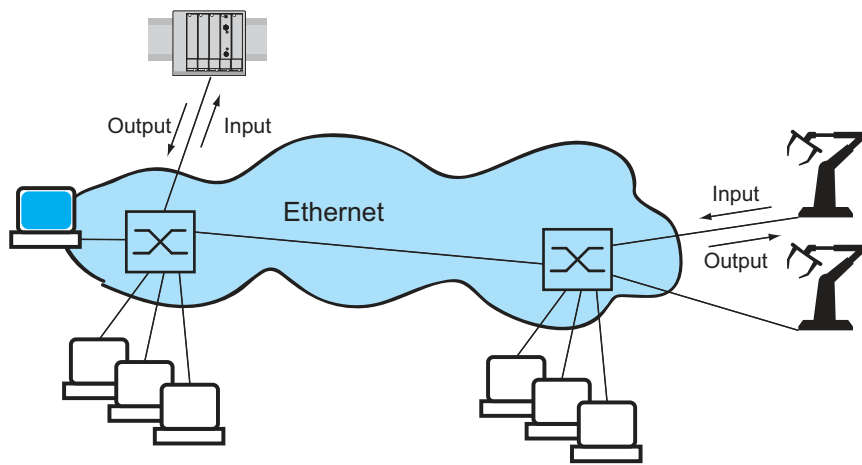


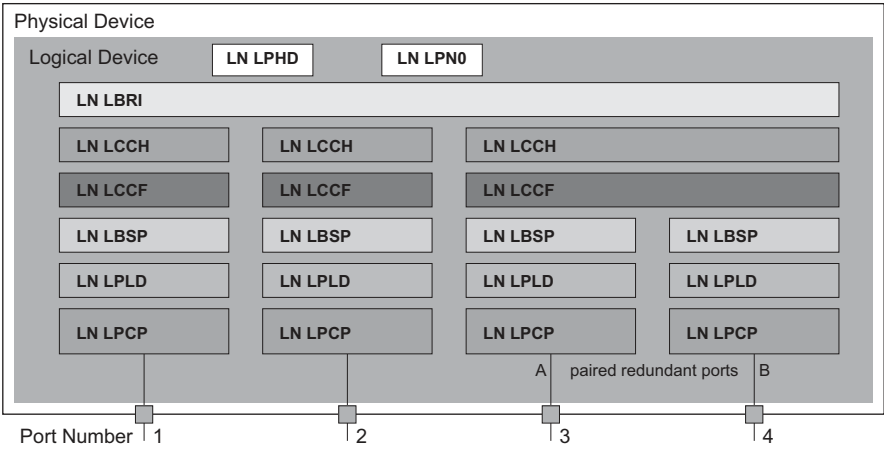








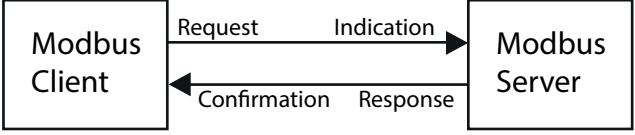






| |
|--|
| |
| |







A series of horizontal lines for writing, consisting of 30 lines in total. The lines are evenly spaced and extend across the width of the page.

| |
|--|
| |
| |



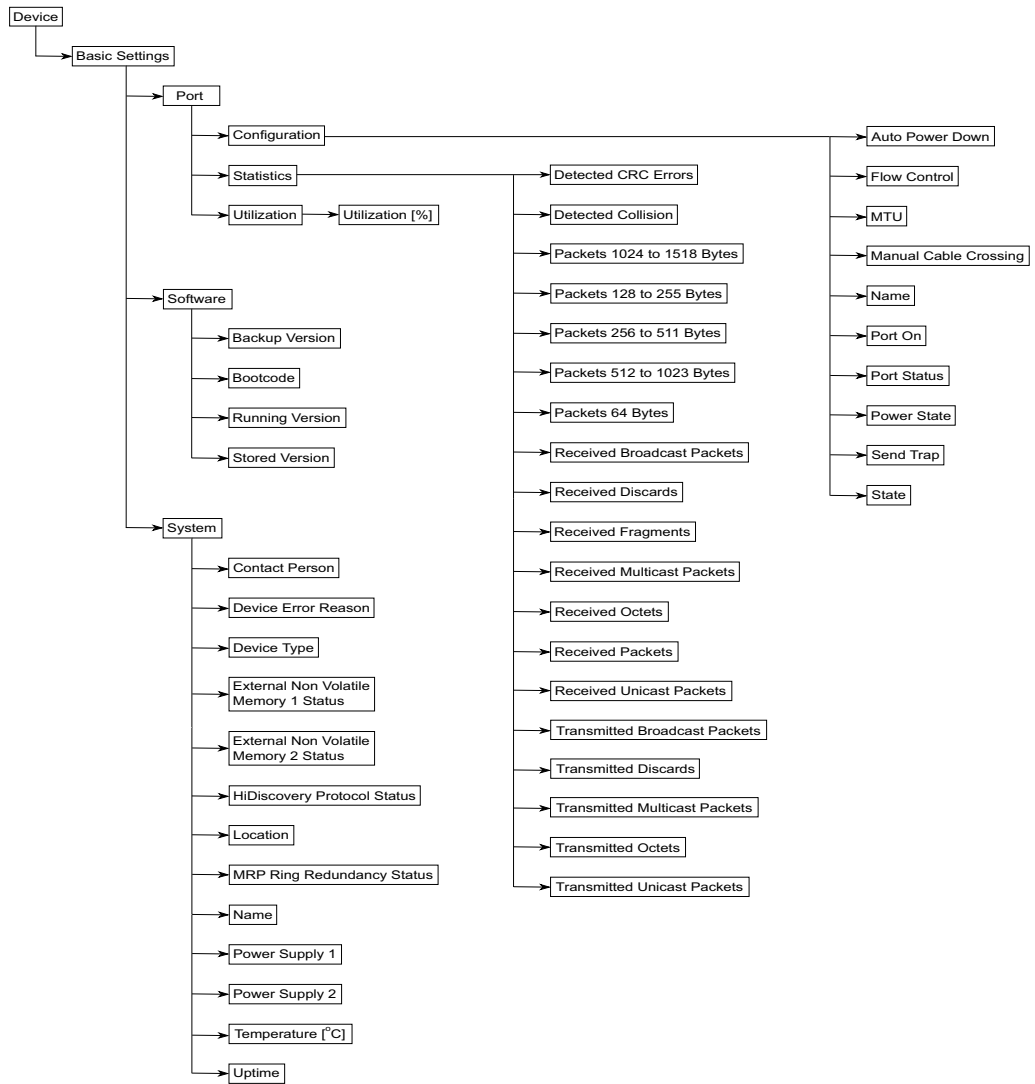
田+

✓

✓











⌘+



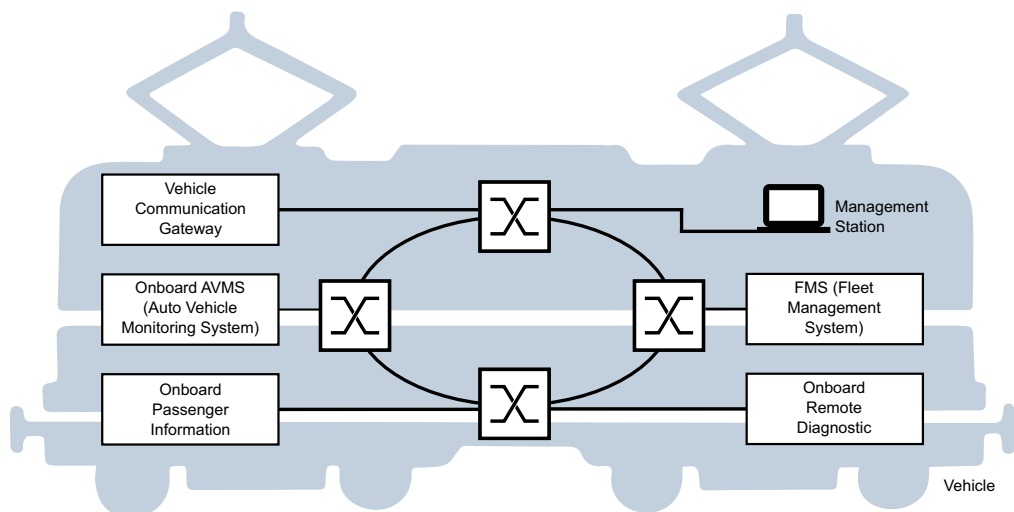


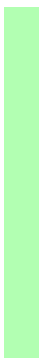
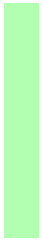
0x



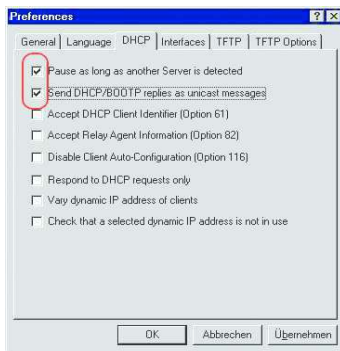


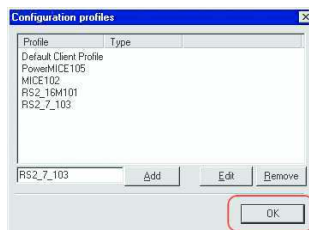
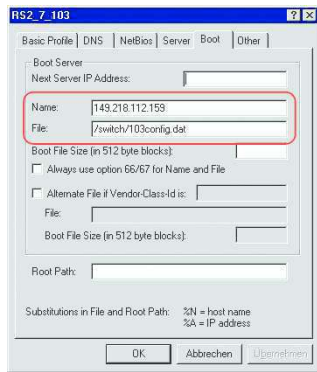
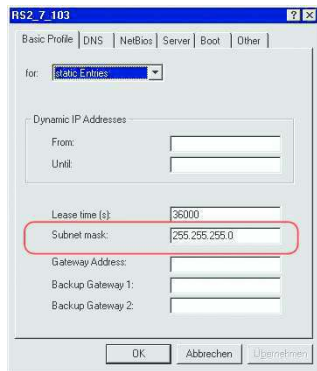
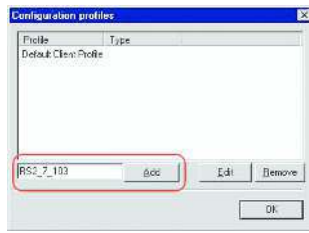


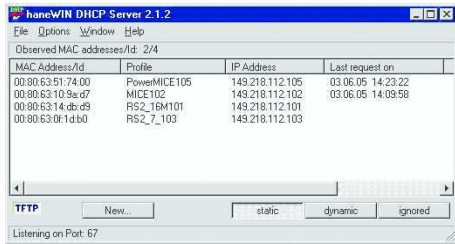
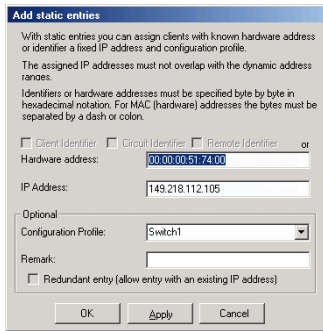
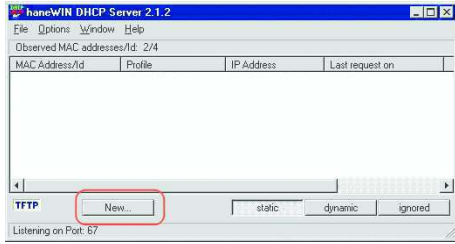
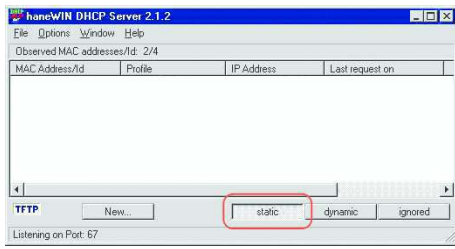


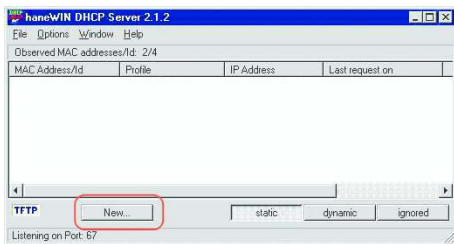
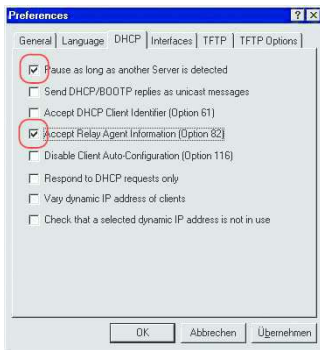












Add static entries

With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

Client Identifier Circuit Identifier Remote Identifier or

Hardware address:

IP Address:

Optional

Configuration Profile:

Remark:

Redundant entry (allow entry with an existing IP address)

OK Apply Cancel

Add static entries

With static entries you can assign clients with known hardware address or identifier a fixed IP address and configuration profile.

The assigned IP addresses must not overlap with the dynamic address ranges.

Identifiers or hardware addresses must be specified byte by byte in hexadecimal notation. For MAC (hardware) addresses the bytes must be separated by a dash or colon.

Client Identifier Circuit Identifier Remote Identifier or

Hardware address:

IP Address:

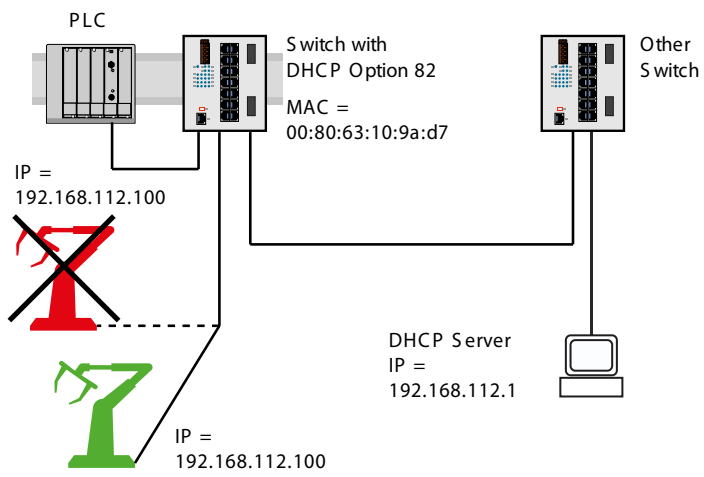
Optional

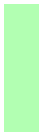
Configuration Profile:

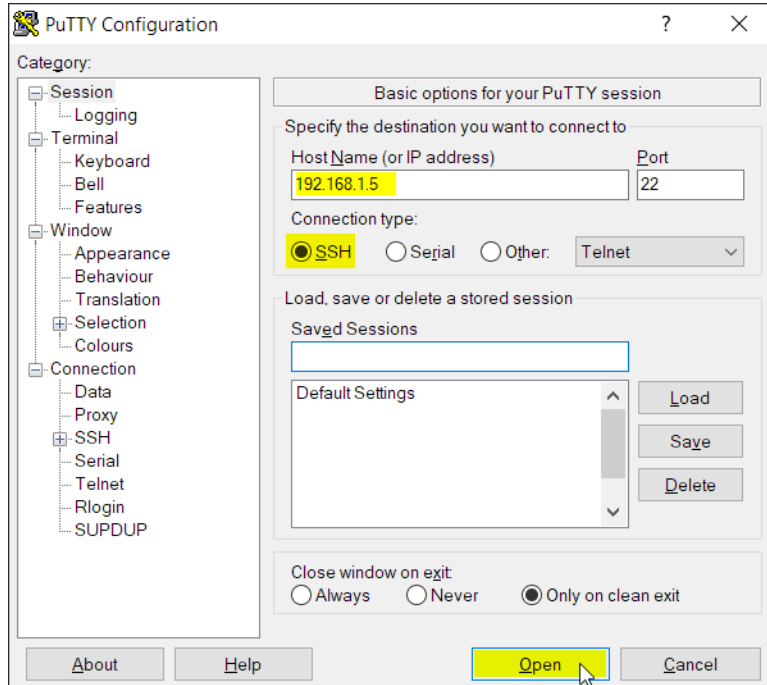
Remark:

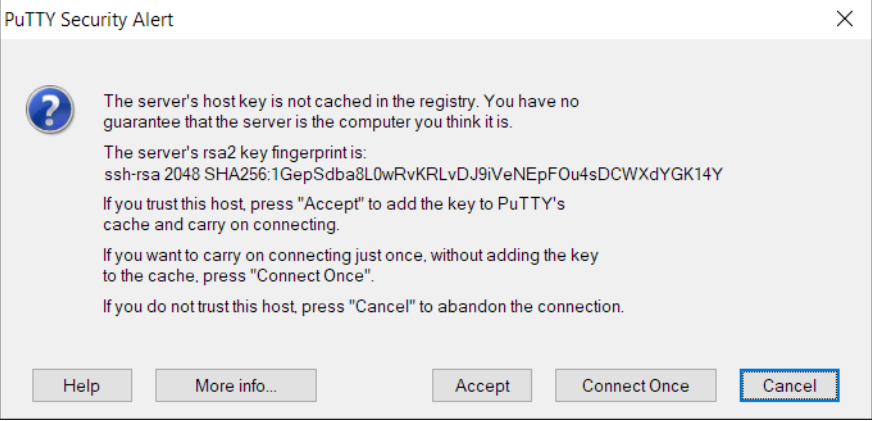
Redundant entry (allow entry with an existing IP address)

OK Apply Cancel





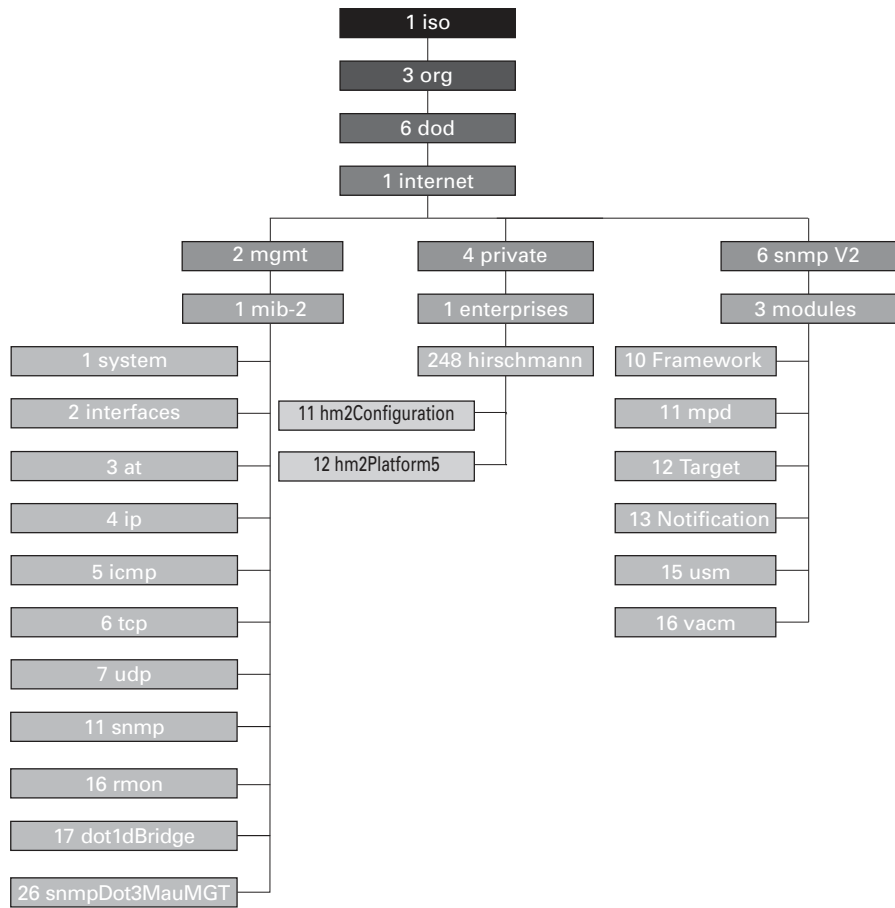




















Lined writing area consisting of multiple horizontal black lines for text entry.



HIRSCHMANN

A **BELDEN** BRAND